PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-179609
(43)Date of publication of application : 27.06.2003

(51)Int.Cl. H04L 12/28
G06F 15/00
H04L 9/32
H04Q 7/38

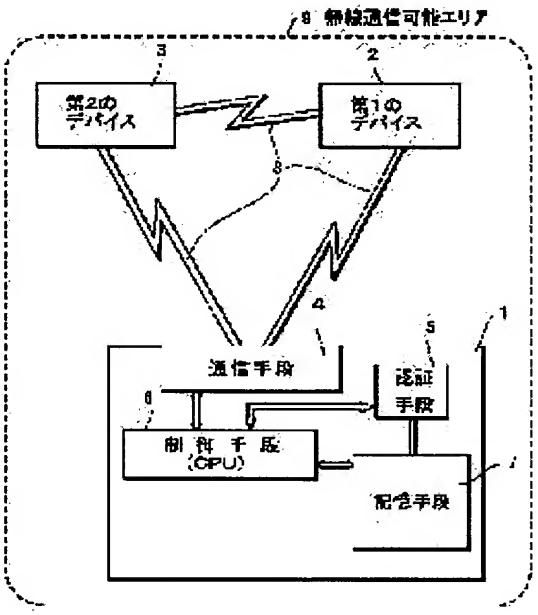
(21)Application number : 2002-202072
(22)Date of filing : 11.07.2002

(71)Applicant : TAIKO DENKI CO LTD
E WITH U:KK
(72)Inventor : MAEDA MIKIO
MATSUDA SHUNSUKE
MIMURO SATORU

(30)Priority
Priority number : 2001243039 Priority date : 09.08.2001 Priority country : JP

(54) COMMUNICATION AUTHENTICATION DEVICE AND COMMUNICATION AUTHENTICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a communication authentication device connected with variously constituted mobile terminals and house appliances of a Bluetooth (R) system by radio communication, for authenticating whether or not the connection of individual devices within the radio communication area is permitted before the mobile terminals and the house appliances of the Bluetooth (R) system start 'data communication'.
SOLUTION: The communication authentication device authenticates radio connection among the devices such as a portable terminal, a portable telephone, a personal computer and digital audio equipment, and is provided with a communication means performing the radio connection with the respective devices, an authentication means discriminating whether or not to enable transmission or reception of data between the devices, a control means controlling the communication means and the authentication means, and a storage means storing the data for authentication control used in the control means.



LEGAL STATUS

[Date of request for examination] 12.07.2002
[Date of sending the examiner's decision of rejection] 24.05.2005
[Kind of final disposal of application other than

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－179609
(P2003－179609A)
(43)公開日　平成15年６月27日(2003.6.27)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｈ０４Ｌ　12/28	３００	Ｈ０４Ｌ　12/28	３００Ｚ	５Ｂ０８５
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｃ	５Ｊ１０４
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ａ	５Ｋ０３３
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ	５Ｋ０６７

審査請求　有　　請求項の数17　ＯＬ　（全 27 頁）

(21)出願番号　特願2002－202072(P2002－202072)

(22)出願日　平成14年７月11日(2002.7.11)

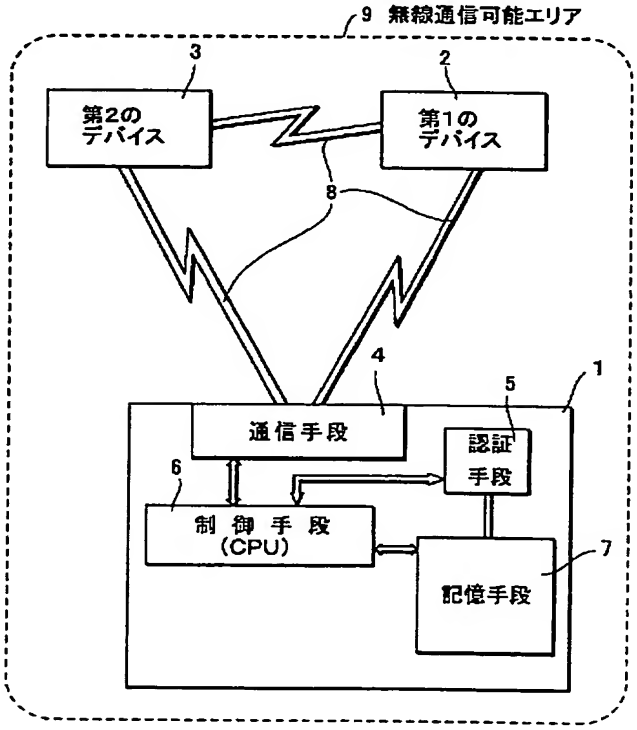
(31)優先権主張番号　特願2001－243039(P2001－243039)
(32)優先日　平成13年８月９日(2001.8.9)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000205122
大宏電機株式会社
東京都大田区矢口３丁目７番３号
(71)出願人　500529850
株式会社イーウィズユー
東京都品川区南大井６－17－17　ＦＩＮＥビル
(72)発明者　前田　幹夫
東京都大田区矢口３丁目７番３号　大宏電機株式会社内
(74)代理人　100087745
弁理士　清水　善▲廣▼　（外２名）

最終頁に続く

(54)【発明の名称】　通信認証装置及び通信認証方法

(57)【要約】
【課題】さまざまに構成されたブルートゥース方式のモバイル端末や家電装置と、無線通信で接続され、ブルートゥース方式のモバイル端末や家電装置が「データ通信」を開始する前に、個々の装置がその無線通信エリア内での接続許可されたものかどうか認証する通信認証装置を提供することを目的とする。
【解決手段】通信認証装置は、携帯端末、携帯電話、パーソナルコンピュータ、デジタル音響機器等のデバイス間の無線接続を認証する通信認証装置であって、それぞれの前記デバイスと無線接続を行う通信手段と、前記デバイス間のデータの送信又は受信を可能とするか否か判別する認証手段と、前記通信手段と前記認証手段とを制御する制御手段と、前記制御手段で使用する認証制御用データを記憶する記憶手段とを有することを特徴とする。



【特許請求の範囲】

【請求項１】　携帯端末、携帯電話、パーソナルコンピュータ、デジタル音響機器等のデバイス間の無線接続を認証する通信認証装置であって、それぞれの前記デバイスと無線接続を行う通信手段と、前記デバイス間のデータの送信又は受信を可能とするか否か判別する認証手段と、前記通信手段と前記認証手段とを制御する制御手段と、前記制御手段で使用する認証制御用データを記憶する記憶手段とを有することを特徴とする通信認証装置。

【請求項２】　前記記憶手段には、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして記憶することを特徴とする請求項１に記載の通信認証装置。

【請求項３】　前記記憶手段の内部メモリに管理対象となるデバイスの情報を入力する入力手段と、前記ネットワークの通信状態や前記入力手段からの入力情報を表示する表示手段とを有することを特徴とする請求項１に記載の通信認証装置。

【請求項４】　前記制御手段に接続され、外部から起動ができる起動手段を備えたことを特徴とする請求項１に記載の通信認証装置。

【請求項５】　前記制御手段に接続され、あらかじめ決めた位置でのみ制御動作を行うための位置情報検出手段を備えたことを特徴とする請求項１に記載の通信認証装置。

【請求項６】　前記制御手段に接続され、使用者が設定した時刻や一定時間のみ制御手段からの通信命令や認証命令を動作させるタイマー手段を備えたことを特徴とする請求項１に記載の通信認証装置。

【請求項７】　通信認証装置と第１のデバイスと第２のデバイスとがそれぞれ無線通信で接続され、前記第１のデバイスと前記第２のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第１のデバイスから前記第２のデバイスに対して接続要求を出す第１のステップと、第１のステップの後に、前記第２のデバイスが前記第１のデバイスへ接続してよいかどうかを、前記第２のデバイスから前記通信認証装置に対して問い合わせる第２のステップと、第２のステップの後に、前記通信認証装置が前記第１のデバイスの存在を確認する第３のステップと、第３のステップの後に、前記第１のデバイスから前記通信認証装置に対して前記第１のデバイスの存在情報を通知する第４のステップと、第４のステップの後に、前記通信認証装置が前記第１のデバイスの存在を確認した結果を、前記通信認証装置から前記第２のデバイスに対して報告する第５のステップと、第５のステップの後に、前記第１のデバイスと前記第２のデバイスの通信を開始する第６のステップとからなる通信認証方法。

【請求項８】　通信認証装置と第１のデバイスと第２のデバイスとがそれぞれ無線通信で接続され、前記第１のデバイスと前記第２のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第１のデバイスから前記第２のデバイスに対して接続要求を出す第１のステップと、第１のステップの後に、前記第２のデバイスが前記第１のデバイスへ接続してよいかどうかを、前記第２のデバイスから前記通信認証装置に対して問い合わせる第２のステップと、第２のステップの後に、前記通信認証装置と前記第１のデバイスの間で、前記第１のデバイスのアドレス情報又はパスワード情報を送受信することによって前記第１のデバイスを認証する第３のステップと、第３のステップの後に、前記通信認証装置から前記第２のデバイスに対して前記第１のデバイスが通信許可された装置であることを報告する第４のステップと、第４のステップの後に、前記第１のデバイスと前記第２のデバイスの通信を開始する第５のステップとからなる通信認証方法。

【請求項９】　通信認証装置と第１のデバイスと第２のデバイスとがそれぞれ無線通信で接続され、前記第１のデバイスと前記第２のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第１のデバイスから前記第２のデバイスに対して接続要求を出す第１のステップと、第１のステップの後に、前記第２のデバイスが前記第１のデバイスへ接続してよいかどうかを、前記第２のデバイスから前記通信認証装置に対して問い合わせる第２のステップと、第２のステップの後に、前記通信認証装置と前記第２のデバイスの間で、前記第２のデバイスのアドレス情報又はパスワード情報を送受信することによって前記第２のデバイスを認証する第３のステップと、第３のステップの後に、前記通信認証装置と前記第１のデバイスの間で、前記第１のデバイスのアドレス情報又はパスワード情報を送受信することによって前記第１のデバイスを認証する第４のステップと、第４のステップの後に、前記通信認証装置から前記第２のデバイスに対して、前記第１のデバイスが通信許可された装置であることを報告する第５のステップと、第５のステップの後に、前記第１のデバイスと前記第２のデバイスの通信を開始する第６のステップとからなる通信認証方法。

【請求項１０】　通信認証装置と第１のデバイスと第２のデバイスとがそれぞれ無線通信で接続され、前記第１のデバイスと前記第２のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記通信認証装置から前記第２のデバイスに対して情報を要求する第１のステップと、第１のステップの後に、前記第２のデバイスから前記通信認証装置に対して、どのような種類の前記第１のデバイスが利用可能であるか問い合わせる第２のステップと、第２のステップの後に、前記通信認証装置が、利用可能な前記第１のデバイスを検索する第３のステップと、第３のステップの後に、前記第１のデバイスから前記通信認証装置に対して前記第１のデ

バイスの存在情報を通知する第４のステップと、第４のステップの後に、前記通信認証装置が前記第１のデバイスの存在を確認した結果を前記第２のデバイスに報告する第５のステップと、第５のステップの後に、前記第１のデバイスと前記第２のデバイスの通信を開始する第６のステップとからなる通信認証方法。

【請求項１１】　通信認証装置と第１のデバイスと第２のデバイスとがそれぞれ無線通信で接続され、前記第１のデバイスと前記第２のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記通信認証装置から前記第２のデバイスに対して情報を要求する第１のステップと、第１のステップの後に、前記第２のデバイスから前記通信認証装置に対して、どのような種類の前記第１のデバイスが登録されているかを問い合わせる第２のステップと、第２のステップの後に、前記通信認証装置が、利用可能な前記第１のデバイスを検索する第３のステップと、前記第１のデバイスから前記通信認証装置に対して、前記第１のデバイスのアドレス情報又はパスワード情報を送信する第４のステップと、第４のステップの後に、前記通信認証装置が前記第１のデバイスを認証する第５のステップと、第５のステップの後に、前記通信認証装置から前記第２のデバイスに対して、使用する前記第１のデバイスのアドレス情報又はパスワード情報を送信する第６のステップと、第６のステップの後に、前記第１のデバイスと前記第２のデバイスの通信を開始する第７のステップとからなる通信認証方法。

【請求項１２】　通信認証装置と第１のデバイスと第２のデバイスとがそれぞれ無線通信で接続され、前記第１のデバイスと前記第２のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第２のデバイスから前記通信認証装置に対して情報を要求する第１のステップと、第１のステップの後に、前記通信認証装置から前記第２のデバイスに対して前記通信認証装置が記憶管理している前記第１のデバイスに関する情報を含む回答通知を送信する第２のステップと、第２のステップの後に、前記第２のデバイスから特定された前記第１のデバイスに対して確認要求を行う第３のステップと、第３のステップの後に、前記第１のデバイスから前記第２のデバイスに対して、確認結果を送信する第４のステップとからなる通信認証方法。

【請求項１３】　前記認証手段を、使用者個人を特定することが可能な生体情報を読み取って認証する生体情報認証手段とし、前記記憶手段には、使用者個人特有の生体情報を記憶することを特徴とする請求項１に記載の通信認証装置。

【請求項１４】　通信認証装置と第１のデバイスと第２のデバイスとがそれぞれ無線通信で接続され、前記第２のデバイスには外部装置が接続され、前記第１のデバイスと前記第２のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第１のデバイスから前記第２のデバイスに対して接続要求を出す第１のステップと、第１のステップの後に、前記第２のデバイスが前記第１のデバイスへ接続してよいかどうかを、前記第２のデバイスから前記通信認証装置に対して問い合わせる第２のステップと、第２のステップの後に、前記第１のデバイスの所有者が前記通信認証装置の所有者であり、かつ前記通信認証装置が所有者本人の持ち物である証明を、前記通信認証装置に搭載された生体情報認証手段を用いて認証する第３のステップと、第３のステップの後に、前記第３のステップの認証結果が正しければ、前記認証結果を前記通信認証装置から前記第２のデバイスを経由して、前記第２のデバイスに接続されている外部装置に送信する第４のステップと、第４のステップの後に、前記外部装置から前記第２のデバイスを経由して、前記通信認証装置へ通信許可通知を送信する第５のステップと、第５のステップの後に、前記第１のデバイスと前記第２のデバイスの通信を開始する第６のステップとからなることを特徴とする通信認証方法。

【請求項１５】　前記第５のステップの後に、前記第２のデバイスと通信を開始するのが、前記第２のデバイスに接続された第３のデバイスであることを特徴とする請求項１４に記載の通信認証方法。

【請求項１６】　第１のデバイスと第２のデバイスが無線または有線接続され、通信認証装置と第２のデバイスとが無線通信で接続され、前記第２のデバイスには外部装置が接続され、前記第１のデバイスと前記第２のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第１のデバイスから前記第２のデバイスに対して接続要求を出す第１のステップと、第１のステップの後に、前記第２のデバイスが前記第１のデバイスへ接続してよいかどうかを、前記第２のデバイスから前記通信認証装置に対して問い合わせる第２のステップと、第２のステップの後に、前記第１のデバイスの所有者が前記通信認証装置の所有者であり、かつ前記通信認証装置が所有者本人の持ち物である証明を、前記通信認証装置に搭載された生体情報認証手段を用いて認証する第３のステップと、第３のステップの後に、前記第３のステップの認証結果が正しければ、前記認証結果を前記通信認証装置から前記第２のデバイスを経由して、前記第２のデバイスに接続されている外部装置に送信する第４のステップと、第４のステップの後に、前記外部装置から前記第２のデバイスに対して、データを送信する第５のステップとからなることを特徴とする通信認証方法。

【請求項１７】　通信認証装置と第２のデバイスとが無線通信で接続され、前記第２のデバイスには外部装置が接続され、前記第２のデバイスの動作制御を前記外部装置から行う許可を前記通信認証装置で認証する通信認証方法であって、前記通信認証装置が所有者本人の持ち物

である証明を、前記通信認証装置に搭載された生体情報認証手段を用いて認証する第１のステップと、第１のステップの後に、前記第１のステップの認証結果が正しければ、前記認証結果を前記通信認証装置から前記第２のデバイスを経由して、前記第２のデバイスに接続されている外部装置に送信する第２のステップと、第２のステップの後に、前記外部装置から前記第２のデバイスに対して許可データを送信する第３のステップと、第３のステップの後に、前記外部装置から前記第２のデバイスに対して送信された許可データに基づいて前記第２のデバイスが動作を開始する第４のステップとからなることを特徴とする通信認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、携帯端末、携帯電話、パーソナルコンピュータ、デジタル音響機器等のデバイス間の無線接続を認証する通信認証装置及び通信認証方法に関する。

【０００２】

【従来の技術】近年、インターネットの普及やマルチメディアの発展にともなって、情報ネットワーク技術が飛躍的に進歩し、携帯端末、携帯電話、パーソナルコンピュータ、これらの周辺機器、又はデジタル音響機器等の情報通信装置や情報家電装置が、パーソナルコンピュータを中心としたネットワーク上で利用されることが多くなっている。これらの情報通信装置や情報家電装置は、携帯性を重視する必要性から、機能を必要最小限にとどめ、それぞれの機器をコードを用いて接続することで、機能向上を図ったり、データ転送を行っている。しかし、コードを用いた接続では、コードを紛失したり、探し回らなければならない不都合を生じたり、コード配線による煩わしさがあった。このような状況の中で、ワイヤレスによって接続可能な機器が提案され、多くの企業は社内での無線通信によるデータ共有を推進し始め、個人生活においても、家庭内での情報家電装置間のワイヤレス化や、ショッピングなど屋外における生活シーンにおいても携帯端末による電子決裁や情報収集手段として、さまざまな携帯型ワイヤレス通信装置が提案されてきている。比較的近距離の無線通信の手段としては、現在一般使用段階にある無線ＬＡＮと、将来的に普及が見込まれているブルートゥースとがある。しかし、どちらの通信方法も、ケーブルを接続しなければ、ほぼ１００％他者にデータを盗まれない有線通信と比較すると、無線通信は比較的広範囲の空中を電波が飛び回ることから、無線通信機器の機密管理技術や暗号化技術は必須の課題である。無線ＬＡＮは、有線ＬＡＮの規格であるＩＥＥＥ８０２．１１を拡張したものであり、有線ＬＡＮの主流であるイーサネット（登録商標）（１０ｂａｓｅイーサネット（登録商標））のケーブルを電波で置き換えたものである。よって、イーサネット（登録商標）で

はネットワークに接続されたパソコンや機器を識別するために、それぞれ「ＩＰアドレス」という個別の番号を割り振らなければならず、これは無線ＬＡＮでも同様であり、無線通信を行うパソコンはＩＰアドレスを持たなければならない。このＩＰアドレスをネットワーク機器側から自動的に割り振るようにしたのが、ダイヤルアップルータなどに搭載されている「ＤＨＣＰサーバ機能」であり、現在汎用的に利用されているＯＳには、ＤＨＣＰサーバが発行するアドレスを自動で受け入れるＤＨＣＰクライアント機能を装備している。ルータ機能を持つアクセスポイントを使う場合は、これを有効にしておき、ＩＰアドレスの設定をパソコンに任せる方法と、ＩＰアドレスを手動で設定する方法とがある。また、イーサネット（登録商標）につながるコンピュータのイーサネット（登録商標）ボードには、ＭＡＣアドレス（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ　Ａｄｄｒｅｓｓ）という固有の物理アドレスが付いている。ＭＡＣアドレスはイーサネット（登録商標）であれば６バイト長で、先頭の３バイトはベンダコードとしてＩＥＥＥ（米国電気電子学会）が管理／割り当てを行なっている。残り３バイトは各ベンダで独自に重複しないように管理しているコードなので、結果として、世界中で同じ物理アドレスを持つイーサネット（登録商標）ボードは存在せず、すべて異なるアドレスが割り当てられている。イーサネット（登録商標）ではこのアドレスを元にしてフレームの送受信を行っている。ＭＡＣアドレスは ハードウェアアドレスとも呼ばれ、ＴＣＰ／ＩＰのネットワークに接続する場合、ネットワーク管理者が前もってＴＣＰ／ＩＰの設定をする必要がある。よって、無線ＬＡＮ接続が可能な機器を、無線通信有効範囲内に持ち込んだとしても、ＭＡＣアドレスやＴＣＰ／ＩＰの設定等が必要となるので、個人の無線ＬＡＮ環境においては、使用者本人が把握することになり、会社等の無線ＬＡＮ環境においては、ネットワーク管理者の管理下に置かれるので、機密保持手段のひとつとなり得る。一方ブルートゥースが対象とするモバイル端末とは、業務用端末からコンシューマ製品に至るまで幅広いモバイル端末を想定しており、複雑な装置やＯＳ上の設定の必要がなく、誰もが簡単に利用できるものとなっている。例を挙げると、ブルートゥースに対応したモバイル端末なら、近くにデータ・アクセス・ポイント（インターネット・ステーション）　さえあればケーブルなしでインターネット接続が可能となったり、ブルートゥース搭載の携帯電話なら、パソコンの近くに置いておくだけでワイヤレス・モデムとしても利用可能となる。また、会議室にブルートゥース対応機器を持ち込むだけで、同席者のブルートゥース対応機器と自動的にピアツーピア・ネットワークを構成し、データやファイルなど互いの情報を必要に応じて無線で手軽に交換可能となり、個人使用としては、帰宅後入室と同時に手持ちのモバイル端末と自宅のパソコ

ンや、その他のハンドヘルド機器、携帯電話などの間でブルートゥース接続が自動的にされ、スケジュールやアドレス帳のようなファイルも自動的に同期化できる。ブルートゥース規格は、データリンク層でデバイス認証と暗号セキュリティ・サービスを定義しているので、ブルートゥースの通信接続方式のセキュリティ面での課題は、安全性を確保できないセキュリティ・プロトコルを組み込んだ装置や、全くセキュリティ・プロトコルを組み込んでいない装置との無線接続である。また、セキュリティのためにグループ外の装置を受け付けない無線ネットワークであると、新たな装置が、その無線通信エリア内に入ってきても通信が始まらないというブルートゥース本来の趣旨に反する形態になってしまう。また、この新たな機器をブルートゥース機器として使用するための登録作業に複雑なＩＤやパスワードが必要になってくるという結果になる。また、現在のパスワードの一般的な運用方法は、仕事の形態においては、仕事用のノートパソコン等をモバイルパソコンとして、オフィスや自宅以外に持ち出している。そのため、機密性の高いデータを保存しているパソコンは、その内部データの機密保持の手段として、電源立ち上げ時にパスワードを要求してくる「ＢＩＯＳによるパワーオン・パスワード」や、ファイルを読む時にパスワードを要求してくる「ハードディスク・パスワード」や、専用の暗号化ソフトを利用してのファイル暗号化など様々な方法をとっている。つまり、複数のパスワードを使用するのであるが、パスワードの性格として、使用者に関係のある誕生日や電話番号等、他人が容易に知り得る文字列は通常使わない。実際のところは、使用者とは何の関係もない無意味な長い文字列を覚えておいて、機密解除作業ごとに異なるパスワードを入力するという作業となっている。このように複雑なパスワードであると、使用者は忘れないために手帳等にメモを取る場合が多く、パスワード自体を機密管理しなければならないという本来の仕事から離れた手間のかかる作業に時間や神経を使っているのが実状である。

【０００３】

【発明が解決しようとする課題】将来的に普及が見込まれているブルートゥース方式のモバイル端末や家電装置などは、業務用端末からコンシューマ製品、一般家電製品に至るまで幅広い製品群を想定しており、複雑な装置やＯＳ上の設定の必要なく誰もが簡単に利用できるものとなっているので、例えば、無線通信エリア内に持ち込んだモバイル端末の通信環境下では、認証していない他人のモバイル端末が、エリア内のマスターである使用者の意に反して勝手にネットワークに接続されていたり、通信中のデータ内にある機密情報や個人情報を他人に故意に盗み見られる可能性があり、このような無防備な無線通信エリアでは、データ通信を開始する時に通信装置間での通信方式や装置の認証が必要である。この認証方法としては、パスワード入力による認証があるが、操作

が容易でないと、「誰もが簡単に利用できる」ことがメリットであるブルートゥース方式の装置の便利性を損ねてしまう結果となる。そこで、ある一定の条件のもとでは容易にネットワークを構築し、なおかつセキュリティも強固な通信認証方法が求められている。

【０００４】そこで本発明は、さまざまに構成されたブルートゥース方式のモバイル端末や家電装置と、無線通信で接続され、ブルートゥース方式のモバイル端末や家電装置が「データ通信」を開始する前に、個々の装置がその無線通信エリア内での接続許可されたものかどうか認証する通信認証装置を提供することを目的とする。

【０００５】

【課題を解決するための手段】請求項１記載の本発明の通信認証装置は、携帯端末、携帯電話、パーソナルコンピュータ、デジタル音響機器等のデバイス間の無線接続を認証する通信認証装置であって、それぞれの前記デバイスと無線接続を行う通信手段と、前記デバイス間のデータの送信又は受信を可能とするか否か判別する認証手段と、前記通信手段と前記認証手段とを制御する制御手段と、前記制御手段で使用する認証制御用データを記憶する記憶手段とを有することを特徴とする。請求項２記載の本発明は、請求項１に記載の通信認証装置において、前記記憶手段には、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして記憶することを特徴とする。請求項３記載の本発明は、請求項１に記載の通信認証装置において、前記記憶手段の内部メモリに管理対象となるデバイスの情報を入力する入力手段と、前記ネットワークの通信状態や前記入力手段からの入力情報を表示する表示手段とを有することを特徴とする。請求項４記載の本発明は、請求項１に記載の通信認証装置において、前記制御手段に接続され、外部から起動ができる起動手段を備えたことを特徴とする。請求項５記載の本発明は、請求項１に記載の通信認証装置において、前記制御手段に接続され、あらかじめ決めた位置でのみ制御動作を行うための位置情報検出手段を備えたことを特徴とする。請求項６記載の本発明は、請求項１に記載の通信認証装置において、前記制御手段に接続され、使用者が設定した時刻や一定時間のみ制御手段からの通信命令や認証命令を動作させるタイマー手段を備えたことを特徴とする。請求項７記載の本発明の通信認証方法は、通信認証装置と第１のデバイスと第２のデバイスとがそれぞれ無線通信で接続され、前記第１のデバイスと前記第２のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第１のデバイスから前記第２のデバイスに対して接続要求を出す第１のステップと、第１のステップの後に、前記第２のデバイスが前記第１のデバイスへ接続してよいかどうかを、前記第２のデバイスから前記通信認証装置に対して問い合わせる第２のステップと、第２のステップの後に、前記通信認証

装置が前記第１のデバイスの存在を確認する第３のステップと、第３のステップの後に、前記第１のデバイスから前記通信認証装置に対して前記第１のデバイスの存在情報を通知する第４のステップと、第４のステップの後に、前記通信認証装置が前記第１のデバイスの存在を確認した結果を、前記通信認証装置から前記第２のデバイスに対して報告する第５のステップと、第５のステップの後に、前記第１のデバイスと前記第２のデバイスの通信を開始する第６のステップとからなることを特徴とする。請求項８記載の本発明の通信認証方法は、通信認証装置と第１のデバイスと第２のデバイスとがそれぞれ無線通信で接続され、前記第１のデバイスと前記第２のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第１のデバイスから前記第２のデバイスに対して接続要求を出す第１のステップと、第１のステップの後に、前記第２のデバイスが前記第１のデバイスへ接続してよいかどうかを、前記第２のデバイスから前記通信認証装置に対して問い合わせる第２のステップと、第２のステップの後に、前記通信認証装置と前記第１のデバイスの間で、前記第１のデバイスのアドレス情報又はパスワード情報を送受信することによって前記第１のデバイスを認証する第３のステップと、第３のステップの後に、前記通信認証装置から前記第２のデバイスに対して前記第１のデバイスが通信許可された装置であることを報告する第４のステップと、第４のステップの後に、前記第１のデバイスと前記第２のデバイスの通信を開始する第５のステップとからなることを特徴とする。請求項９記載の本発明の通信認証方法は、通信認証装置と第１のデバイスと第２のデバイスとがそれぞれ無線通信で接続され、前記第１のデバイスと前記第２のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第１のデバイスから前記第２のデバイスに対して接続要求を出す第１のステップと、第１のステップの後に、前記第２のデバイスが前記第１のデバイスへ接続してよいかどうかを、前記第２のデバイスから前記通信認証装置に対して問い合わせる第２のステップと、第２のステップの後に、前記通信認証装置と前記第２のデバイスの間で、前記第２のデバイスのアドレス情報又はパスワード情報を送受信することによって前記第２のデバイスを認証する第３のステップと、第３のステップの後に、前記通信認証装置と前記第１のデバイスの間で、前記第１のデバイスのアドレス情報又はパスワード情報を送受信することによって前記第１のデバイスを認証する第４のステップと、第４のステップの後に、前記通信認証装置から前記第２のデバイスに対して、前記第１のデバイスが通信許可された装置であることを報告する第５のステップと、第５のステップの後に、前記第１のデバイスと前記第２のデバイスの通信を開始する第６のステップとからなることを特徴とする。請求項１０記載の本発明の通信認証方法は、通信認

証装置と第１のデバイスと第２のデバイスとがそれぞれ無線通信で接続され、前記第１のデバイスと前記第２のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記通信認証装置から前記第２のデバイスに対して情報を要求する第１のステップと、第１のステップの後に、前記第２のデバイスから前記通信認証装置に対して、どのような種類の前記第１のデバイスが利用可能であるか問い合わせる第２のステップと、第２のステップの後に、前記通信認証装置が、利用可能な前記第１のデバイスを検索する第３のステップと、第３のステップの後に、前記第１のデバイスから前記通信認証装置に対して前記第１のデバイスの存在情報を通知する第４のステップと、第４のステップの後に、前記通信認証装置が前記第１のデバイスの存在を確認した結果を前記第２のデバイスに報告する第５のステップと、第５のステップの後に、前記第１のデバイスと前記第２のデバイスの通信を開始する第６のステップとからなることを特徴とする。請求項１１記載の本発明の通信認証方法は、通信認証装置と第１のデバイスと第２のデバイスとがそれぞれ無線通信で接続され、前記第１のデバイスと前記第２のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記通信認証装置から前記第２のデバイスに対して情報を要求する第１のステップと、第１のステップの後に、前記第２のデバイスから前記通信認証装置に対して、どのような種類の前記第１のデバイスが登録されているかを問い合わせる第２のステップと、第２のステップの後に、前記通信認証装置が、利用可能な前記第１のデバイスを検索する第３のステップと、前記第１のデバイスから前記通信認証装置に対して、前記第１のデバイスのアドレス情報又はパスワード情報を送信する第４のステップと、第４のステップの後に、前記通信認証装置が前記第１のデバイスを認証する第５のステップと、第５のステップの後に、前記通信認証装置から前記第２のデバイスに対して、使用する前記第１のデバイスのアドレス情報又はパスワード情報を送信する第６のステップと、第６のステップの後に、前記第１のデバイスと前記第２のデバイスの通信を開始する第７のステップとからなることを特徴とする。請求項１２記載の本発明の通信認証方法は、通信認証装置と第１のデバイスと第２のデバイスとがそれぞれ無線通信で接続され、前記第１のデバイスと前記第２のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第２のデバイスから前記通信認証装置に対して情報を要求する第１のステップと、第１のステップの後に、前記通信認証装置から前記第２のデバイスに対して前記通信認証装置が記憶管理している前記第１のデバイスに関する情報を含む回答通知を送信する第２のステップと、第２のステップの後に、前記第２のデバイスから特定された前記第１のデバイスに対して確認要求を行う第３のステップと、第３のステップの後

に、前記第１のデバイスから前記第２のデバイスに対して、確認結果を送信する第４のステップとからなることを特徴とする。請求項１３記載の本発明は、請求項１に記載の通信認証装置において、前記認証手段を、使用者個人を特定することが可能な生体情報を読み取って認証する生体情報認証手段とし、前記記憶手段には、使用者個人特有の生体情報を記憶することを特徴とする。請求項１４記載の本発明の通信認証方法は、通信認証装置と第１のデバイスと第２のデバイスとがそれぞれ無線通信で接続され、前記第２のデバイスには外部装置が接続され、前記第１のデバイスと前記第２のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第１のデバイスから前記第２のデバイスに対して接続要求を出す第１のステップと、第１のステップの後に、前記第２のデバイスが前記第１のデバイスへ接続してよいかどうかを、前記第２のデバイスから前記通信認証装置に対して問い合わせる第２のステップと、第２のステップの後に、前記第１のデバイスの所有者が前記通信認証装置の所有者であり、かつ前記通信認証装置が所有者本人の持ち物である証明を、前記通信認証装置に搭載された生体情報認証手段を用いて認証する第３のステップと、第３のステップの後に、前記第３のステップの認証結果が正しければ、前記認証結果を前記通信認証装置から前記第２のデバイスを経由して、前記第２のデバイスに接続されている外部装置に送信する第４のステップと、第４のステップの後に、前記外部装置から前記第２のデバイスを経由して、前記通信認証装置へ通信許可通知を送信する第５のステップと、第５のステップの後に前記第１のデバイスと前記第２のデバイスの通信を開始する第６のステップとからなることを特徴とする。請求項１５記載の本発明の通信認証方法は、請求項１４に記載の通信認証方法において、前記第５のステップの後に、前記第２のデバイスと通信を開始するのが、前記第２のデバイスに接続された第３のデバイスであることを特徴とする。請求項１６記載の本発明の通信認証方法は、第１のデバイスと第２のデバイスが無線または有線接続され、通信認証装置と第２のデバイスとが無線通信で接続され、前記第２のデバイスには外部装置が接続され、前記第１のデバイスと前記第２のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第１のデバイスから前記第２のデバイスに対して接続要求を出す第１のステップと、第１のステップの後に、前記第２のデバイスが前記第１のデバイスへ接続してよいかどうかを、前記第２のデバイスから前記通信認証装置に対して問い合わせる第２のステップと、第２のステップの後に、前記第１のデバイスの所有者が前記通信認証装置の所有者であり、かつ前記通信認証装置が所有者本人の持ち物である証明を、前記通信認証装置に搭載された生体情報認証手段を用いて認証する第３のステップと、第３のステップの後に、前記第３のステップ

の認証結果が正しければ、前記認証結果を前記通信認証装置から前記第２のデバイスを経由して、前記第２のデバイスに接続されている外部装置に送信する第４のステップと、第４のステップの後に、前記外部装置から前記第２のデバイスに対して、データを送信する第５のステップとからなることを特徴とする。請求項１７記載の本発明の通信認証方法は、通信認証装置と第２のデバイスとが無線通信で接続され、前記第２のデバイスには外部装置が接続され、前記第２のデバイスの動作制御を前記外部装置から行う許可を前記通信認証装置で認証する通信認証方法であって、前記通信認証装置が所有者本人の持ち物である証明を、前記通信認証装置に搭載された生体情報認証手段を用いて認証する第１のステップと、第１のステップの後に、前記第１のステップの認証結果が正しければ、前記認証結果を前記通信認証装置から前記第２のデバイスを経由して、前記第２のデバイスに接続されている外部装置に送信する第２のステップと、第２のステップの後に、前記外部装置から前記第２のデバイスに対して許可データを送信する第３のステップと、第３のステップの後に、前記外部装置から前記第２のデバイスに対して送信された許可データに基づいて前記第２のデバイスが動作を開始する第４のステップとからなることを特徴とする。

【０００６】

【発明の実施の形態】本発明の第１の実施の形態による通信認証装置は、それぞれのデバイスと無線接続を行う通信手段と、デバイス間のデータの送信又は受信を可能とするか否か判別する認証手段と、通信手段と認証手段とを制御する制御手段と、制御手段で使用する認証制御用データを記憶する記憶手段とを有するものである。本実施の形態によれば、無線通信が可能なエリア内にある２台以上の通信装置とは別に存在する通信認証装置によって、エリア内にある２台以上の通信装置を互いに「データ通信」可能とするか否かの制御をすることができる。従って、あらかじめ通信認証装置に認証制御用データが記憶されていれば、この通信認証装置をエリア内に持ち込むことにより、通信認証装置内部の記憶手段に記憶された認証制御用データに登録されている通信装置を接続して使用可能とすることができる。

【０００７】本発明の第２の実施の形態は、第１の実施の形態による通信認証装置において、記憶手段には、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして記憶するものである。本実施の形態によれば、使用者自身に由縁のある氏名、生年月日、電話番号、電子メールアドレス、免許証番号等の情報をパスワードとして登録するので、忘却する危険性が少なく、パスワードを書き留める必要がない。

【０００８】本発明の第３の実施の形態は、第１の実施の形態による通信認証装置において、記憶手段の内部メ

モリに管理対象となるデバイスの情報を入力する入力手段と、ネットワークの通信状態や入力手段からの入力情報を表示する表示手段とを有するものである。本実施の形態によれば、無線通信が可能なエリア内にある２台以上のデバイスとは別に存在する通信認証装置によって、エリア内にある２台以上のデバイスを互いに「データ通信」可能とするか否かの制御をすることができる。従って、あらかじめ通信認証装置に認証制御用データが記憶されていれば、この通信認証装置をエリア内に持ち込むことにより、通信認証装置内部の記憶手段に記憶された認証制御用データに登録されているデバイスを接続して使用可能とすることができる。さらに、入力手段として釦や表示手段として表示窓を設けることにより、移動先の通信エリアでの急な認証作業が可能となる。

【０００９】本発明の第４の実施の形態は、第１の実施の形態による通信認証装置において、制御手段に接続され、外部から起動ができる起動手段を備えたものである。本実施の形態によれば、据え置かれた通信認証装置の場合でも、使用者の入室を検知したり、鍵の挿入を検知したり、その他装置の起動に同期して、通信認証装置を起動できるので、通信認証装置の存在を気にすることなく快適にセキュリティを保持できる。従って、例えば自動車等にキーレスエントリーで搭乗した時や、鍵を使用してエンジンスタートした時に、通信認証装置を起動して携帯電話とカーナビゲーション装置をブルートゥースで接続して通信をし、携帯電話から基地局経由で地図情報を受信し、カーナビゲーション装置に送信したりできる。

【００１０】本発明の第５の実施の形態は、第１の実施の形態による通信認証装置において、制御手段に接続され、あらかじめ決めた位置でのみ制御動作を行うための位置情報検出手段を備えたものである。本実施の形態によれば、通信認証装置の内部の位置情報検出手段により、使用者があらかじめ設定した地球上の座標に居る場合のみ各デバイスの使用が可能となる。従って、決まった場所でのみ通信認証を行うので、強固なセキュリティを保持できる。

【００１１】本発明の第６の実施の形態は、第１の実施の形態による通信認証装置において、制御手段に接続され、使用者が設定した時刻や一定時間のみ制御手段からの通信命令や認証命令を動作させるタイマー手段を備えたものである。本実施の形態によれば、通信認証装置の内部のタイマー手段により、使用者があらかじめ設定した時刻や、使用者が設定した時間経過後、あるいは使用者が設定した時間内で各デバイスの使用が可能となる。従って、第三者の通信認証装置の無断使用による通信認証を防止できる。

【００１２】本発明の第７の実施の形態による通信認証方法は、第１のデバイスから第２のデバイスに対して接続要求を出す第１のステップと、第１のステップの後

に、第２のデバイスが第１のデバイスへ接続してよいかどうかを、第２のデバイスから通信認証装置に対して問い合わせる第２のステップと、第２のステップの後に、通信認証装置が第１のデバイスの存在を確認する第３のステップと、第３のステップの後に、第１のデバイスから通信認証装置に対して第１のデバイスの存在情報を通知する第４のステップと、第４のステップの後に、通信認証装置が第１のデバイスの存在を確認した結果を、通信認証装置から第２のデバイスに対して報告する第５のステップと、第５のステップの後に、第１のデバイスと第２のデバイスの通信を開始する第６のステップとからなるものである。本実施の形態によれば、通信認証装置を無線通信エリア内に持ち込むことにより、はじめて第１のデバイスと第２のデバイスが、通信認証装置が介在することによってデータ通信を開始するので、第３者からの勝手なアクセスによる接続での機密データの流出が生じない。

【００１３】本発明の第８の実施の形態による通信認証方法は、第１のデバイスから第２のデバイスに対して接続要求を出す第１のステップと、第１のステップの後に、第２のデバイスが第１のデバイスへ接続してよいかどうかを、第２のデバイスから通信認証装置に対して問い合わせる第２のステップと、第２のステップの後に、通信認証装置と第１のデバイスの間で、第１のデバイスのアドレス情報又はパスワード情報を送受信することによって第１のデバイスを認証する第３のステップと、第３のステップの後に、通信認証装置から第２のデバイスに対して第１のデバイスが通信許可された装置であることを報告する第４のステップと、第４のステップの後に、第１のデバイスと第２のデバイスの通信を開始する第５のステップとからなるものである。本実施の形態によれば、通信認証装置を無線通信エリア内に持ち込み、第１のデバイスをパスワード等の認証手段を用いることにより、はじめて第１のデバイスと第２のデバイスがデータ通信を開始するので、第３者からの勝手なアクセスによる接続での機密データの流出が生じない。

【００１４】本発明の第９の実施の形態による通信認証方法は、第１のデバイスから第２のデバイスに対して接続要求を出す第１のステップと、第１のステップの後に、第２のデバイスが第１のデバイスへ接続してよいかどうかを、第２のデバイスから通信認証装置に対して問い合わせる第２のステップと、第２のステップの後に、通信認証装置と第２のデバイスの間で、第２のデバイスのアドレス情報又はパスワード情報を送受信することによって第２のデバイスを認証する第３のステップと、第３のステップの後に、通信認証装置と第１のデバイスの間で、第１のデバイスのアドレス情報又はパスワード情報を送受信することによって第１のデバイスを認証する第４のステップと、第４のステップの後に、通信認証装置から第２のデバイスに対して、第１のデバイスが通信

許可された装置であることを報告する第５のステップと、第５のステップの後に、第１のデバイスと第２のデバイスの通信を開始する第６のステップとからなるものである。本実施の形態によれば、通信認証装置を無線通信エリア内に持ち込み、第２のデバイスをパスワード等の認証手段を用いることにより、はじめて第１のデバイスと第２のデバイスがデータ通信を開始するので、第３者からの勝手なアクセスによる接続での機密データの流出が生じない。

【００１５】本発明の第１０の実施の形態による通信認証方法は、通信認証装置から第２のデバイスに対して情報を要求する第１のステップと、第１のステップの後に、第２のデバイスから通信認証装置に対して、どのような種類の第１のデバイスが利用可能であるか問い合わせる第２のステップと、第２のステップの後に、通信認証装置が、利用可能な第１のデバイスを検索する第３のステップと、第３のステップの後に、第１のデバイスから通信認証装置に対して第１のデバイスの存在情報を通知する第４のステップと、第４のステップの後に、通信認証装置が第１のデバイスの存在を確認した結果を第２のデバイスに報告する第５のステップと、第５のステップの後に、第１のデバイスと第２のデバイスの通信を開始する第６のステップとからなるものである。本実施の形態によれば、通信認証装置を無線通信エリア内に持ち込み、第２のデバイスの使用により第１のデバイスと接続すべき第２のデバイスを認証し、その認証情報を第１のデバイスに送信することにより、はじめて第１のデバイスと第２のデバイスがデータ通信を開始するので、第３者からの勝手なアクセスによる接続での機密データの流出が生じない。

【００１６】本発明の第１１の実施の形態による通信認証方法は、通信認証装置から第２のデバイスに対して情報を要求する第１のステップと、第１のステップの後に、第２のデバイスから通信認証装置に対して、どのような種類の第１のデバイスが登録されているかを問い合わせる第２のステップと、第２のステップの後に、通信認証装置が、利用可能な第１のデバイスを検索する第３のステップと、第１のデバイスから通信認証装置に対して、第１のデバイスのアドレス情報又はパスワード情報を送信する第４のステップと、第４のステップの後に、通信認証装置が第１のデバイスを認証する第５のステップと、第５のステップの後に、通信認証装置から第２のデバイスに対して、使用する第１のデバイスのアドレス情報又はパスワード情報を送信する第６のステップと、第６のステップの後に、第１のデバイスと第２のデバイスの通信を開始する第７のステップとからなるものである。本実施の形態によれば、通信認証装置を無線通信エリア内に持ち込み、まず第１のデバイスを確定し、次に第２のデバイスの使用により第１のデバイスと接続すべき第２のデバイスを認証し、その認証情報を第１のデバイスに送信することにより、はじめて第１のデバイスと第２のデバイスがデータ通信を開始するので、第３者からの勝手なアクセスによる接続での機密データの流出が生じない。

【００１７】本発明の第１２の実施の形態による通信認証方法は、第２のデバイスから通信認証装置に対して情報を要求する第１のステップと、第１のステップの後に、通信認証装置から第２のデバイスに対して通信認証装置が記憶管理している第１のデバイスに関する情報を含む回答通知を送信する第２のステップと、第２のステップの後に、第２のデバイスから特定された第１のデバイスに対して確認要求を行う第３のステップと、第３のステップの後に、第１のデバイスから第２のデバイスに対して、確認結果を送信する第４のステップとからなるものである。本実施の形態によれば、通信認証装置を無線通信エリア内に持ち込み、第１のデバイスと第２のデバイスを認証した後、第２のデバイスから第１のデバイスに送信したデータの正誤を第１のデバイスの使用者が確認し、第２のデバイスに結果報告することにより、はじめて第２のデバイスが別の通信回線を使用して第１のデバイスから送られてきたデータを転送し計算するので、クレジットカードや金額情報等の個人情報が、第３者からの勝手なアクセスによる接続によって外部に流出しない。

【００１８】本発明の第１３の実施の形態は、第１の実施の形態による通信認証装置において、認証手段を、使用者個人を特定することが可能な生体情報を読み取って認証する生体情報認証手段とし、記憶手段には、使用者個人特有の生体情報を記憶するものである。本実施の形態によれば、使用者自身を確定する人物認証に、使用者本人の指紋や角膜や遺伝子などの生体情報を用いて認証するため、通信認証装置の所有者や、通信認証装置を含むシステムの所有者と、現在の使用者が同一人物である確証がより正確に取れる。また、ほぼ１００％の確立で同一の生体情報は存在しないため、使用者の特定精度を向上するためのパスワード等の認証キーを複数必要なくなり、結果として使用者の認証操作が簡単になる。更に、認証対象が１つの生体情報であっても十分に個人を特定できるため、人物認証するための通信認証装置の小型化や、認証アルゴリズムの簡略化が容易に図れる。

【００１９】本発明の第１４の実施の形態による通信認証方法は、第１のデバイスから第２のデバイスに対して接続要求を出す第１のステップと、第１のステップの後に、第２のデバイスが第１のデバイスへ接続してよいかどうかを、第２のデバイスから通信認証装置に対して問い合わせる第２のステップと、第２のステップの後に、第１のデバイスの所有者が通信認証装置の所有者であり、かつ通信認証装置が所有者本人の持ち物である証明を、通信認証装置に搭載された生体情報認証手段を用いて認証する第３のステップと、第３のステップの後に、

第３のステップの認証結果が正しければ、認証結果を通信認証装置から第２のデバイスを経由して、第２のデバイスに接続されている外部装置に送信する第４のステップと、第４のステップの後に、外部装置から前記第２のデバイスを経由して、通信認証装置へ通信許可通知を送信する第５のステップと、第５のステップの後に、第１のデバイスと第２のデバイスの通信を開始する第６のステップとからなるものである。本実施の形態によれば、外部装置を含む第１と第２のデバイスと通信認証装置で構成されるシステム、あるいは第１のデバイスと通信認証装置が使用者自身の所有物であることの証明を、システム使用開始時に使用者自身の生体情報（指紋、角膜、遺伝子等）を用いて行うため、システム全体あるいは個々のデバイスからの機密情報の流出が生じない。また、第５のステップの後に、通信認証装置から第２のデバイスへ通信許可を送信し、その許可情報によって第１のデバイスと第２のデバイスの通信を開始するようにすれば、更に強固に通信の機密を保つことができる。なお、第５のステップにおける通信データの流れを第２のデバイスが監視しておいて、第２のデバイスから確実に通信許可が通信認証装置に送り出されたことを検出して、その検出結果をもって第１のデバイスと第２のデバイスの通信を開始する方法であっても十分に通信機密を保持できる。

【００２０】本発明の第１５の実施の形態による通信認証方法は、本発明の第１４の実施の形態による通信認証方法において、第５のステップの後に、第２のデバイスと通信を開始するのが、第２のデバイスに接続された第３のデバイスであるものである。本実施の形態によれば、外部装置を含む第１と第２と第３デバイスと通信認証装置で構成されるシステム、あるいは第１のデバイスと通信認証装置が使用者自身の所有物であることの証明を、システム使用開始時に使用者自身の生体情報（指紋、角膜、遺伝子等）を用いて行うため、システム全体あるいは個々のデバイスからの機密情報の流出が生じない。また、第１のデバイスが機密性の高い操作系機器で、第３のデバイスは公共性の高い表示系機器というような自由度の高いシステムを構築できる。もちろん、第３のデバイスも個人専用機器であり、通信認証装置によってセキュリティをかけた装置であってもよい。

【００２１】本発明の第１６の実施の形態による通信認証方法は、第１のデバイスから第２のデバイスに対して接続要求を出す第１のステップと、第１のステップの後に、第２のデバイスが第１のデバイスへ接続してよいかどうかを、第２のデバイスから通信認証装置に対して問い合わせる第２のステップと、第２のステップの後に、第１のデバイスの所有者が通信認証装置の所有者であり、かつ通信認証装置が所有者本人の持ち物である証明を、通信認証装置に搭載された生体情報認証手段を用いて認証する第３のステップと、第３のステップの後に、

第３のステップの認証結果が正しければ、認証結果を前記通信認証装置から第２のデバイスを経由して、第２のデバイスに接続されている外部装置に送信する第４のステップと、第４のステップの後に、外部装置から前記第２のデバイスに対して、データを送信する第５のステップとからなるものである。本実施の形態によれば、外部装置を含む第１と第２のデバイスと通信認証装置で構成されるシステム、あるいは第１のデバイスと通信認証装置が使用者自身の所有物であることの証明を、システム使用開始時に使用者自身の生体情報（指紋、角膜、遺伝子等）を用いて行うため、システム全体あるいは個々のデバイスからの機密情報の流出が生じない。また、第１のデバイスが使用者自身の所有物であるという証明は、第１のデバイスと通信認証装置間で完了しているので、第２のデバイスや第２のデバイスに接続された外部装置内部で新たに個人情報等（クレジットカード番号等も含む）の機密データを照会する必要がない。

【００２２】本発明の第１７の実施の形態による通信認証方法は、通信認証装置が所有者本人の持ち物である証明を、前記通信認証装置に搭載された生体情報認証手段を用いて認証する第１のステップと、第１のステップの後に、第１のステップの認証結果が正しければ、認証結果を通信認証装置から第２のデバイスを経由して、第２のデバイスに接続されている外部装置に送信する第２のステップと、第２のステップの後に、外部装置から第２のデバイスに対して許可データを送信する第３のステップと、第３のステップの後に、外部装置から第２のデバイスに対して送信された許可データに基づいて第２のデバイスが動作を開始する第４のステップとからなるものである。本実施の形態によれば、外部装置を含む第２のデバイスと通信認証装置で構成されるシステム、あるいは第２のデバイスと通信認証装置、あるいは通信認証装置のみが使用者自身の所有物であることの証明を、システム使用開始時に使用者自身の生体情報（指紋、角膜、遺伝子等）を用いて行うため、システム全体あるいは個々のデバイスからの機密情報の流出が生じない。また、第２のデバイスが使用者自身の所有物であるという証明は、第２のデバイスと通信認証装置間で完了しているので、第２のデバイスや第２のデバイスに接続された外部装置内部で新たに個人情報等の機密データを照会する必要がない。

【００２３】

【実施例】以下本発明の一実施例による通信認証装置について図面に基づいて説明する。図１は一対のデバイスと最も簡略な通信認証装置の接続形態であり、通信認証装置を機能実現手段で表したブロック図である。まず、通信認証装置の基本機能について図１を用いて説明する。第１のデバイス２と、第２のデバイス３と、通信認証装置１とは、それぞれ通信回線８によって近距離無線通信で接続されている。近距離無線通信としては例えば

ブルートゥースを用いることができる。ここでブルートゥースは、２．４ギガヘルツのＩＳＭバンドで動作する無線通信技術である。図１において、通信認証装置１の通信手段４は、第１のデバイス２と、第２のデバイス３と、通信回線８を介して繋がっている。ここで、第１のデバイス２と第２のデバイス３とは、すぐに通信を開始するものではなく、通信認証装置１内部の記憶手段７に記憶された通信認証用データ（パスワードなど）や通信構成に従って認証手段５で認証が実行され、制御手段６によって通信手段４を制御してはじめて、第１のデバイス２と第２のデバイス３とのデータ通信が開始される。ここで通信認証装置１は、例えばＩＣカードのように極めて軽量小型（薄型）の携帯できるものが好ましいが、据え置き型であってもよいし、同様の機能を追加機能として備えたパソコン、携帯電話、ＰＨＳ、又はＰＤＡ等の携帯端末であってもよい。なお、通信機能を有する携帯端末の場合には、あらかじめ認証手段５を備えていなくても、認証手段５として必要なプログラムをサーバから通信回線を介してダウンロードして利用することもできる。例えばＪａｖａ（登録商標）アプレットをWWWサーバからダウンロードして利用する。また、デバイス２およびデバイス３は通信機能を備えた装置であって、コンピュータ周辺機器であるキーボード、マウス、プリンター、イメージスキャナ、ターミナルアダプタや、モバイル機器であるデジタルカメラ、ナビゲーション装置、パームＯＳコンピュータや、一般家電機器をネットワーク対応にした情報家電装置や携帯電話など、通信機能によりさまざまに拡張される電気製品を含むデバイスである。なお、認証手段５は、使用者の指紋、角膜、遺伝子等の人体固有の生体情報を検出して認証を行うものであってもよい。

【００２４】図２は、本発明の一実施例による通信認証装置を機能実現手段で表したブロック図であり、図１の通信認証装置１に追加機能として、表示手段１０と入力手段１１を設けたものである。表示手段１０には通信状態や、入力手段１１によって入力したパスワードなどを表示する。ここで、表示手段１０としては、液晶表示が一般的であるが、プラズマやＣＲＴ等他の方式の表示でもよい。また、入力手段１１としては、キーボードやテンキーボードが一般的であるが、タッチパネルや音声認識入力などでも実現できる。なお、認証手段５は、使用者の指紋、角膜、遺伝子等の人体固有の生体情報を検出して認証を行うものであってもよい。

【００２５】図３は、本発明の一実施例による通信認証装置を機能実現手段で表したブロック図であり、さらに他の追加機能を含むものである。以下、特に追加機能について説明する。リムーバブルメモリ手段１２は、前述の記憶手段７の内、記憶領域の全てか、又は一部の領域をリムーバブル領域で構成したもので、通信認証装置１以外の装置（例えばパソコン）で、認証用データを作成

するができる。ホストインターフェイス手段１３は、外部にホストコンピュータ５１を接続して記憶手段７内部の認証用データを追加、削除、訂正などのメンテナンスを行い、あるいは通信認証装置１自身が正常に動作しているか検査するなどのために設けたものである。起動手段１４は、鍵５２の挿入によって通信認証装置１をスタンバイ状態から起動動作させるものであり、特に携帯型の通信認証装置１である場合のバッテリー消費を考慮したものである。ここで鍵５２は図３では接触挿入型で記載しているが、キーレスエントリーシステムなど非接触型鍵であってもよい。位置検出手段１５は、通信認証装置１の位置を検出するものであり、位置情報によって通信認証装置１をスタンバイ状態から起動動作させたり、通信認証の開始や停止を行える。位置情報検出方法としては、ＧＰＳやPHSによる位置検出方法があるが、その他の方法であってもよい。また、位置検出地点の誤差除去ができるもの（Ｄ－ＧＰＳ）であってもよい。タイマー手段１６は、認証時間の設定、一定時間経過後の通信認証の開始又は停止などの用途で使用する。このタイマー手段１６の設定によって、無人での通信認証装置１の使用や、通信認証装置１の所有者が不在の時間のセキュリティが確保できる。外部入力端子１７は、通信認証装置１の外部にキーボード５３等の入力装置を接続するための端子である。表示出力手段１８は、通信認証装置１の外部に、モニター５４などの表示手段を接続するためのものである。この表示出力手段１８は、外部出力端子１７と同様に、モニター５４を接続することによって、設定変更などのメンテナンスを行うことができる。

【００２６】本実施例では、制御手段における認証制御用データを記憶している記憶手段７の内、記憶領域の全てか、又は一部をリムーバブル領域で構成したリムーバブルメモリ手段１２を備えることで、通信認証装置１の制御手段６における認証制御用データを、あらかじめ他のパーソナルコンピュータやパームＯＳコンピュータなどを用いて作成し、その後で通信認証装置１に格納することができる。従って、比較的容易にデバイスの登録や次回接続のネットワーク構成に合わせたデバイスの再構成などのメンテナンスができる。また本実施例では、通信手段４と認証手段５とを制御する制御手段６に接続され、記憶手段７の内部メモリへの管理対象デバイスの情報の入力や、ネットワークの通信状態を表示するためのホストコンピュータ５１を接続するホストインターフェイス手段１３を備えることで、通信認証装置１の制御手段６における認証制御用データを、有線又は無線で接続されたホストコンピュータ５１を用いて作成したり、次回接続のネットワーク構成に合わせたデバイスの再構成などのメンテナンスや、通信状態が正常に動作できているか否かの確認を容易に行うことができる。また本実施例では、外部から接触又は非接触の起動ができる起動手段１４を備えることで、据え置かれた通信認証装置１の

場合でも、使用者の入室を検知したり、鍵５２の挿入を検知したり、その他装置の起動に同期して、通信認証装置１を起動できるので、通信認証装置１の存在を気にすることなく快適にセキュリティを保持できる。従って、例えば自動車等にキーレスエントリーで搭乗した時や、鍵を使用してエンジンスタートした時に、通信認証装置を起動して携帯電話とカーナビゲーション装置をブルートゥースで接続して通信をし、携帯電話から基地局経由で地図情報を受信し、カーナビゲーション装置に送信することができる。

【００２７】また本実施例では、位置情報検出手段１５を備えているので、使用者があらかじめ設定した地球上の座標に居る場合のみ各デバイスの使用が可能となるように設定することができる。このように、決まった場所でのみ通信認証を行うことで、強固なセキュリティを保持できる。また本実施例では、使用者が設定した時刻や一定時間のみ制御手段６からの通信命令や認証命令を動作させるタイマー手段１６を備えることで、使用者があらかじめ設定した時刻や、使用者が設定した時間経過後、あるいは使用者が設定した時間内で各デバイスの使用が可能となるように設定することができる。従って、第三者の通信認証装置１の無断使用による通信認証を防止できる。また本実施例では、外部入力装置５３によって入力するための外部入力端子１７を備えることで、ホストコンピュータの接続などの手間を掛けることなく、通信認証装置１の制御手段６における認証制御用データを入力して、記憶手段７の内部メモリに格納することができるので、比較的容易にデバイスの登録や次回接続のネットワーク構成に合わせたデバイスの再構成などのメンテナンスができる。従って、キーボード等を接続することによってのみ、通信認証装置の設定を変更できるので、第三者の通信認証装置の無断使用による通信認証を防止できる。また本実施例では、外部モニター５４に表示するための表示出力端子１８を備えることで、表示機能のない通信認証装置１に外部モニター５４をつないで、通信状態確認時、デバイス登録時、メンテナンス時など使用者が必要な時のみ内部情報や通信形態の表示を行うことができる。従って、通信認証装置の管理者（使用者）のみ、内部に記憶されている通信形態や、現在の通信状況を閲覧できるので、第三者の通信認証装置の無断使用による通信認証を防止できる。なお、認証手段５は、使用者の指紋、角膜、遺伝子等の人体固有の生体情報を検出して認証を行うものであってもよい。なお、本実施例の通信認証装置１は、それぞれの機能を説明する上で、それぞれを別構成で説明したが、全ての手段を備えていてもよく、目的に応じた一部の手段を備えているものであってもよい。

【００２８】図４と図５は、本発明の一実施例による通信認証方法を示すブロック図である。なお、以下の実施例で説明する通信認証装置１は、図１から図３で既に説明した通信認証装置の構成を適用することができる。図４は第１のデバイス２がヘッドホンであり、第２のデバイス３がミュージックプレーヤであって、両者の接続認証を通信認証装置１で行うものである。ヘッドホン２がミュージックプレーヤ３に接続要求を出すと（Ｓ４０１）、ミュージックプレーヤ３は通信認証装置１に対して接続してよいデバイスかどうか確認問い合わせをする（Ｓ４０２）。通信認証装置１はヘッドホン２の存在をチェックし（Ｓ４０３）、ヘッドホン２から存在情報の返送をもらう（Ｓ４０４）。そして、通信認証装置１はミュージックプレーヤ３に対してヘッドホン２の存在を通知し（Ｓ４０５）、ミュージックプレーヤ３はヘッドホン２との接続を完了する（Ｓ４０６）。従って、ミュージックプレーヤ３で再生する音楽をヘッドホン２によって受信して利用することができる。

【００２９】図５は、第１のデバイス２が小型送受話装置であり、第２のデバイス３が携帯電話であって、両者の接続認証を通信認証装置１で行うものである。ここで携帯電話３は、通信網５５を経由して他の携帯電話、又はその他の通信機器と接続して音声その他のデータの送受信を行うものである。小型送受話装置２が携帯電話３に接続要求を出すと（Ｓ５０１）、携帯電話３は通信認証装置１に対して接続してよいデバイスかどうか確認問い合わせをする（Ｓ５０２）。通信認証装置１は小型送受話装置２の存在をチェックし（Ｓ５０３）、小型送受話装置２から存在情報の返送をもらう（Ｓ５０４）。通信認証装置１は携帯電話３に小型送受話装置２の存在を通知し（Ｓ５０５）、携帯電話３は小型送受話装置２との接続を完了する（Ｓ５０６）。従って、携帯電話３で送受信するデータを小型送受話装置２によって送受信して利用することができる。

【００３０】図６から図１０は、本発明の他の実施例による通信認証方法を示すブロック図である。図６は第１のデバイス２が音楽データ記録装置であり、第２のデバイス３がデジタルラジオであって、両者の接続認証を通信認証装置１で行うものである。音楽データ記録装置２がデジタルラジオ３に接続要求を出し（Ｓ６０１）、デジタルラジオ３は通信認証装置１に対して接続してよいデバイスかどうか確認問い合わせをする（Ｓ６０２）。通信認証装置１は音楽データ記録装置２の装置アドレスをチェックし（Ｓ６０３）、音楽データ記録装置２から装置アドレスを返送させる（Ｓ６０４）。通信認証装置１は返送された装置アドレスが、通信認証装置１内部の記憶手段７に記憶されているアドレスであるか照合する（Ｓ６０５）。通信認証装置１はデジタルラジオ３に音楽データ記録装置２へのデータ送信を許可し（Ｓ６０６）、デジタルラジオ３は放送局５４から受信した音楽データを音楽データ記録装置２へ送信する（Ｓ６０７）。

【００３１】図７は第１のデバイス２が携帯端末装置で

あり、第２のデバイス３がファイルストレージ装置であって、両者の接続認証を通信認証装置１で行うものである。携帯端末装置２がファイルストレージ装置３にファイル要求を出し（Ｓ７０１）、ファイルストレージ装置３は通信認証装置１に対して接続してよいデバイスかどうか確認問い合わせをする（Ｓ７０２）。通信認証装置１は携帯端末装置２の装置アドレスをチェックし（Ｓ７０３）、携帯端末装置２から装置アドレスを返送させる（Ｓ７０４）。通信認証装置１は返送された装置アドレスが、通信認証装置内部の記憶手段７に記憶されているアドレスであるか照合する（Ｓ７０５）。通信認証装置１はファイルストレージ装置３に携帯端末装置２へファイルオープンを許可し（Ｓ７０６）、ファイルストレージ装置３は携帯端末装置２へファイルオープンして送信する（Ｓ７０７）。

【００３２】図８は第１のデバイス２が電話装置であり、第２のデバイス３が公衆網用ゲートウェイであって、両者の接続認証を通信認証装置１で行うものである。電話装置２が公衆網用ゲートウェイ３に接続要求を出し（Ｓ８０１）、公衆網用ゲートウェイ３は通信認証装置１に対して接続してよいデバイスかどうか確認問い合わせをする（Ｓ８０２）。通信認証装置１は電話装置２の装置アドレスをチェックし（Ｓ８０３）、電話装置２から装置アドレスを返送させる（Ｓ８０４）。通信認証装置１は返送された装置アドレスが、通信認証装置内部の記憶手段７に記憶されているアドレスであるか照合する（Ｓ８０５）。通信認証装置１は公衆網用ゲートウェイ３に電話装置２への接続を許可し（Ｓ８０６）、公衆網用ゲートウェイ３は公衆網５５からの通信を中継して電話装置２へ転送する（Ｓ８０７）。

【００３３】図９は第１のデバイス２が電子メール／Ｗｅｂ端末装置であり、第２のデバイス３がインターネットアクセス装置であって、両者の接続認証を通信認証装置１で行うものである。電子メール／Ｗｅｂ端末装置２がインターネットアクセス装置３に接続要求を出し（Ｓ９０１）、インターネットアクセス装置３は通信認証装置１に対して接続してよいデバイスかどうか確認問い合わせをする（Ｓ９０２）。通信認証装置１は電子メール／Ｗｅｂ端末装置２の装置アドレスをチェックし（Ｓ９０３）、電子メール／Ｗｅｂ端末装置２から装置アドレスを返送させる（Ｓ９０４）。通信認証装置１は返送された装置アドレスが、通信認証装置内部の記憶手段７に記憶されているアドレスであるか照合する（Ｓ９０５）。通信認証装置１はインターネットアクセス装置３に電子メール／Ｗｅｂ端末装置２との接続許可を出し（Ｓ９０６）、インターネット５７からの電子メールやＷｅｂデータを、インターネットアクセス装置３を介して電子メール／Ｗｅｂ端末装置２へ転送する（Ｓ９０７）。

【００３４】図１０は第１のデバイス２が電話装置であり、第２のデバイス３が音声データ記録装置であって、両者の接続認証を通信認証装置１で行うものである。電話装置２が音声データ記録装置３に通話録音要求を出し（Ｓ１０１）、音声データ記録装置３は通信認証装置１に対して接続してよいデバイスかどうか確認問い合わせをする（Ｓ１０２）。通信認証装置１は電話装置２の装置アドレスをチェックし（Ｓ１０３）、電話装置２から装置アドレスを返送させる（Ｓ１０４）。通信認証装置１は返送された装置アドレスが、通信認証装置内部の記憶手段７に記憶されているアドレスであるか照合する（Ｓ１０５）。通信認証装置１は音声データ記録装置３に電話装置２からの音声データの録音許可を出し（Ｓ１０６）、公衆網５５から公衆網用ゲートウェイ５６を経由して電話装置２で交信されている音声データを音声データ記録装置３で録音する（Ｓ１０７）。

【００３５】図１１は、本発明の他の実施例による通信認証方法を示すブロック図である。本実施例は、第１のデバイス２が携帯端末装置であり、第２のデバイス３がインターネットアクセス装置であって、両者の接続認証を通信認証装置１で行うものである。通信認証装置１がインターネットアクセス装置３に情報要求を出し（Ｓ１１１）、インターネットアクセス装置３は通信認証装置１に対してどのような携帯端末装置２に接続可能か問い合わせをする（Ｓ１１２）。通信認証装置１は利用可能な携帯端末装置２を検索し（Ｓ１１３）、携帯端末装置２を使用者が操作する（Ｓ１１４）ことにより、携帯端末装置２から通信認証装置１に装置アドレスが返送される（Ｓ１１５）。通信認証装置１は返送された装置アドレスをインターネットアクセス装置３に通知する（Ｓ１１６）。インターネットアクセス装置３は通知された装置アドレスを持つ携帯端末装置２に対してインターネット５７からの情報を送信する（Ｓ１１７）。

【００３６】図１２は、本発明の他の実施例による通信認証方法を示すブロック図である。本実施例は、第１のデバイス２が携帯端末装置であり、第２のデバイス３がインターネットアクセス装置であって、両者の接続認証を通信認証装置１で行うものである。通信認証装置１がインターネットアクセス装置３に情報要求を出し（Ｓ１１１）、インターネットアクセス装置３は通信認証装置１に対してどのような携帯端末装置２に接続可能か問い合わせをする（Ｓ１１２）。通信認証装置１は利用可能な携帯端末装置２を検索し（Ｓ１１３）、携帯端末装置２を使用者が操作する（Ｓ１１４）ことにより、携帯端末装置２から通信認証装置１に装置アドレスが返送される（Ｓ１１５）。通信認証装置１は返送された装置アドレスが、通信認証装置内部の記憶手段７に記憶されているアドレスであるか照合する（Ｓ１２６）。通信認証装置１は返送された装置アドレスをインターネットアクセス装置３に通知する（Ｓ１２７）。インターネットアクセス装置３は通知された装置アドレスを持つ携帯端末装

置２に対してインターネット５７からの情報を送信する（Ｓ１２８）。

【００３７】図１３は、本発明の他の実施例による通信認証方法を示すブロック図である。本実施例は、第１のデバイス２が携帯電話等の表示機能を持った端末装置であり、第２のデバイス３がレジスター装置であって、両者の接続認証を通信認証装置１で行うものである。レジスター装置３から通信認証装置１に決裁情報を要求し（Ｓ１３１）、通信認証装置１は決裁要求のあったレジスター装置アドレスが、通信認証装置内部の記憶手段７に記憶されているアドレスであるか照合する（Ｓ１３２）。通信認証装置１は、決裁可能である情報（表示を行う表示装置２を特定する情報を含む）をレジスター装置３に通知する（Ｓ１３３）。レジスター装置３は合計金額を、特定された携帯電話２に通知し（Ｓ１３４）、携帯電話２の使用者は合計金額の確認をレジスター装置３に送り（Ｓ１３５）、インターネット５７を介して金融機関等で決裁される。ここで、Ｓ１３１の決裁情報にこれから精算すべき顧客の携帯電話２の装置アドレスを含めて送信し、通信認証装置１では、既に登録済みの顧客であるかの判断により決裁可能かどうかの判断することにより更にセキュリティを強化できる。

【００３８】図１４は、本発明の他の実施例による通信認証方法を示すブロック図である。本実施例は、第１のデバイス２は１台であり、第２のデバイス３が、n台まで複数である構成の通信認証方法である。第２のデバイス３から第１のデバイス２に接続要求を出し（Ｓ１４１）、第１のデバイス２が第２のデバイス３へ接続してよいかどうかを、第１のデバイス２から通信認証装置１へ問い合わせ（Ｓ１４２）、通信認証装置１が第２のデバイス３の存在をチェックし（Ｓ１４３）、第２のデバイス３から装置アドレスを返送する（Ｓ１４４）。通信認証装置１は返送された装置アドレスが、通信認証装置内部の記憶手段７に記憶されているアドレスであるか照合する（Ｓ１４５）。通信認証装置１は第１のデバイス２に対して、第２のデバイス３との接続許可を送り（Ｓ１４６）、第１のデバイス２と第２のデバイス３とのデータ通信が開始される（Ｓ１４７）。以上の通信認証を複数台順次認証していく。また、通信認証装置１にあらかじめ通信形態を登録しておくことによって、ブルートゥース通信に規定されているマスターとスレーブの装置関係の決定もできる。

【００３９】本実施例による通信認証方法は、通信認証装置と無線通信で接続されていて、互いに第１のデバイスと１：１の関係で無線接続されている第２のデバイスから第ｎ（ｎは自然数）のデバイスにおいて、第１のデバイスから第２のデバイスに接続要求を出すステップと、第１のデバイスが第２のデバイスへ接続してよいかどうかを、第１のデバイスから通信認証装置へ問い合わせるステップと、通信認証装置が第２のデバイスの装置

アドレスを確認するステップと、第２のデバイスから装置アドレスを返送するステップと、返送された装置アドレスが通信認証装置内部の記憶手段に記憶されているアドレスであるか照合するステップと、通信認証装置が第１のデバイスに対して、第２のデバイスとの接続許可を送信するステップと、第１のデバイスと第２のデバイスの接続を完了するステップとを有している。そして、第１のデバイスと第２のデバイスの接続が完了するまでのステップを、第ｎのデバイスまで順次繰り返し行うものである。本実施例によれば、無線通信エリア内にある１台の通信認証装置を用いて第１のデバイスと１：１の関係でｎ台まで順次認証していくことができる。また、本実施例によると、会議室に会議参加メンバーの所有するブルートゥースを搭載したモバイルコンピュータが持ち込まれ、会議参加メンバーに資料を配付していく場合などにおいても、強固にセキュリティを保持できる。

【００４０】また本実施例による通信認証方法は、通信認証装置と無線通信で接続されていて、互いに第１のデバイスと１：１の関係で無線接続されている第２のデバイスから第ｎ（ｎは自然数）のデバイスにおいて、第１のデバイスから第２のデバイスに接続要求を出すステップと、第１のデバイスが第２のデバイスへ接続してよいかどうかを、第１のデバイスから通信認証装置へ問い合わせるステップと、通信認証装置が第２のデバイスの装置アドレスを確認するステップと、第２のデバイスから装置アドレスを返送するステップと、返送された装置アドレスが通信認証装置内部の記憶手段に記憶されているアドレスであるか照合するステップと、通信認証装置が第１のデバイスに対して、第２のデバイスとの接続許可を送信するステップと、第１のデバイスと第２のデバイスの接続を完了するステップとを有する。そして、通信認証装置にあらかじめ設定された通信形態に従って、第１のデバイスと第２のデバイスの接続が完了するまでのステップを、第ｎのデバイスまで順次繰り返し行う。本実施例によれば、無線通信エリア内にある１台の通信認証装置を用いて、あらかじめ通信認証装置に設定登録した通信形態に従って、第１のデバイスと１：１の関係でｎ台まで順次認証していくことができる。また、本実施例によると、会議室などであらかじめ設定しておいた通信形態に基づいて、会議参加メンバーの所有するブルートゥースを搭載したモバイルコンピュータを認証していくので、より強固にセキュリティを保持することができる。なお、本実施例では、通信認証を複数台順次認証するとしたが、同時に複数台の認証を行う構成であってもよい。

【００４１】図１５は、本発明の他の実施例による通信認証方法を示すブロック図である。本実施例は、第１のデバイス２は１台であり、第２のデバイス３が、n台まで複数であるが、それぞれのデバイスがブルートゥース通信のマスター装置であり、またそれぞれにスレーブ装

置が複数台接続されている場合の通信認証方法である。第２のデバイス（３から第nのデバイス3n）まで順次接続認証をし（Ｓ１５１）、同時にそれぞれに接続されたスレーブを、通信認証装置１にあらかじめ設定した構成に従ってネットワークから切り離す（Ｓ１５２）。次に、通信認証装置１は第１のデバイス２をマスター装置に選定し（Ｓ１５３）、第１のデバイス２と第２のデバイス（スレーブ装置）３とのデータ通信が開始される。そして第n番目の第２のデバイス（スレーブ装置）３nまでデータ通信を行う。また、通信認証装置１をマスター装置として、第１番目から第n番目の第２のデバイス３をスレーブ装置として通信認証したあとで、スレーブ装置とした第２のデバイス３中の１台を新たなマスター装置として構成してもよい。また、本実施例における通信認証方法は、将来的にウェアブル化されたパーソナルコンピュータをマスター装置として身に付け、その周辺に各種モバイル装置をスレーブ装置として接続した状態の人間が複数名で１つの会議室に集結した場合に、セキュリティを確保しながら、あらかじめ設定した通信形態に容易に移行できる。

【００４２】本実施例による通信認証方法は、通信認証装置が一台設置されていて、第１のデバイスと１：１の関係で無線接続されている第２のデバイスから第ｎ（ｎは自然数）のデバイスからなるネットワークが複数個、同一無線通信エリア内に集結した通信形態を前提とする。そして、集結した各々のネットワークの内、代表の１つのデバイスを、あらかじめ通信認証装置に登録されているアドレス情報に基づいて、集結したネットワークの数と同じか、それ以下の数だけ、順次認証していくステップと、代表の１つのデバイス（認証完了したデバイス）を複数個集めて、あらかじめ通信認証装置に設定しているネットワークを形成するステップと、複数個のデバイスの内、マスターとなる１台を選択認証するステップと、マスターのデバイスと１：１の関係で、その他の代表のデバイスと通信を開始するステップとを有する。本実施例によれば、無線通信エリア内に１台の通信認証装置を設置し、そのエリア内に１：ｎで構成された複数個のネットワークが集結した場合、集結した個々のネットワーク中の１台を、あらかじめ通信認証装置に登録されている装置アドレス情報に基づいて認証し、その認証したデバイスの内の１台をマスターとして、新しく構成されたネットワークの中心装置として通信を開始することができるので、ブルートゥース端末装置等の無秩序な通信を防止できる。

【００４３】図１６は、本発明の他の実施例による通信認証方法を示すブロック図である。本実施例は、第１のデバイス２は１台であり、第２のデバイス３が、n台まで複数であるが、それぞれのデバイスがブルートゥース通信のマスター装置であり、またそれぞれのマスター装置に通信認証装置１台とスレーブ装置が複数台接続され

ている場合の通信認証方法である。本実施例は、複数の通信認証装置間で先に近距離無線通信によって接続し、あらかじめ通信認証装置１に登録されている優先順位情報に基づいて最上位通信認証装置を決定し（Ｓ１６１）、各々の通信認証装置から、最上位通信認証装置に対して各々の通信認証装置に接続されているデバイスの内、代表の１台のデバイスのアドレス情報を通知し（Ｓ１６２）、その他のデバイスはネットワークから切り離す（Ｓ１６３）。最上位通信認証装置は、登録されているアドレス情報と装置構成に基づいてデバイスを順次認証していき（Ｓ１６４）、認証を完了したデバイスの内の１台をマスター装置と指定して（Ｓ１６５）、その他のデバイスをスレーブ装置として通信を開始する（Ｓ１６６）。また、本実施例では、n台全てのデバイスを認証する形態で説明したが、通信認証装置１に設定されているn台よりも少ない台数を認証し、元マスター装置であったデバイスにスレーブ装置として接続されていたデバイスを最終的な通信形態で通信可能にするものであってもよい。また、本実施例における通信認証方法は、将来的にウェアブル化されたパーソナルコンピュータをマスター装置として身に付け、その周辺に通信認証装置と各種モバイル装置をスレーブ装置として接続した状態の人間が複数名で１つの会議室に集結した場合に、セキュリティを確保しながら、あらかじめ設定した通信形態に容易に移行できる。

【００４４】本実施例による通信認証方法は、通信認証装置と無線通信で接続されていて、互いに第１のデバイスと１：１の関係で無線接続されている第２のデバイスから第ｎ（ｎは自然数）のデバイスからなるネットワークが複数個、同一無線通信エリア内に集結した通信形態を前提とする。そして、集結した各々のネットワークの内、代表の１つの通信認証装置を、あらかじめ通信認証装置に登録されている優先順位情報に基づいて最上位通信認証装置として決定するステップと、各々の通信認証装置から、最上位通信認証装置に対して、集結した各々のネットワーク中の代表のデバイスのアドレス情報を通知するステップと、集結した各々のネットワーク中の内、代表の１つのデバイスを、最上位の通信認証装置に登録されているアドレス情報に基づいて、順次認証していくステップと、代表の１つのデバイス（認証完了したデバイス）を複数個を集めて、あらかじめ通信認証装置に設定しているネットワークを形成するステップと、複数個のデバイスの内、マスターとなる１台を選択認証するステップと、マスターのデバイスと、１：１の関係で、その他の代表のデバイスと通信を開始するステップとを有する。本実施例によれば、デバイスｎ台と通信認証装置１台の組み合わせで同一の無線通信エリアに集結した場合に、集結した複数台の通信認証装置の内の１台が、あらかじめ通信認証装置に登録されている優先順位情報に基づいて最上位通信認証装置として決定され、他

の通信認証装置と接続されていたデバイスを装置アドレス情報に基づいて順次認証し、その認証したデバイスの内の１台をマスターとして、新しく構成されたネットワークの中心装置として通信を開始することができるので、ブルートゥース端末装置等の無秩序な通信を防止できる。なお、図４から図１６までのそれぞれの通信認証装置１における認証手段として、使用者の指紋、角膜、遺伝子等の人体固有の生体情報を検出して認証を行う機能を付加することにより、機密保持をより一層強固なものにできる。

【００４５】次に、通信認証装置１のパスワードによる通信認証について、通信認証装置１へのパスワード登録方法とデバイスを認証する際のパスワード解除方法を、図１７から図２２を用いて説明する。図１７から図２２は、本発明の一実施例によるパスワードによる通信認証方法を示すフロー図である。

【００４６】図１７に記載の通信認証方法は、まず使用者がパスワード入力で通信許可をもらう際に、通信認証装置から質問させる形式を、あらかじめ設定しておき（Ｓ１７１）、複数の無線デバイスを、パスワードを用いて登録する時、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして入力し（Ｓ１７２）、入力したパスワードを通信認証装置１のメモリ部７に記憶する（Ｓ１７３）。次に、複数の無線デバイスを通信エリア内で通信可能にする際は、あらかじめ使用者が設定した質問形式で質問される内容の回答を、デバイスから通信認証装置１にデータを入力して送信し（Ｓ１７４）、入力によって回答したデータと通信認証装置１のメモリ部７に記憶された使用者の個人データを比較し（Ｓ１７５）、比較した結果が一致した場合には通信を許可し、複数の無線デバイスを使用可能とする（Ｓ１７６）。Ｓ１７５で不一致の場合には、再度回答を入力して送信し（Ｓ１７４）、入力したデータと通信認証装置１のメモリ部７に記憶された使用者の個人データを比較する（Ｓ１７５）。なお、セキュリティの面から、この不一致の場合の回答回数を所定回数に限ることが好ましい。認証の際の質問形式の設定にあたっては、例えば複数の内の１つのパスワードを質問、複数の内の２つのパスワードを質問、又は複数の内の所定数のパスワードを質問させ、登録されているパスワードの中から質問形式と一致するパスワードが入力された場合に通信を許可する。また、質問形式はデバイス毎に変更し、デバイス特有のパスワードを選択させる場合であってもよい。また通信接続する２つのデバイスによって、複数のパスワードの内の特有のパスワードを選択する場合であってもよい。また、通信の接続時間帯や、エリアによって複数のパスワードの内の特有のパスワードを選択する場合であってもよい。また、パスワードに関して、本実施例では、実際の個人データをパスワードとして入力する場合で説明したが、使用者が設定したユニークな識別番号又は識別記号であってもよい。ここで説明した質問形式の設定、及びパスワードに関しては、本実施例に限らず下記で説明する実施例においても適用できる。

【００４７】本実施例による通信認証方法は、複数の無線デバイスを扱う通信システムにおいて、複数の無線デバイスをパスワードで登録し、しかる後に複数の無線デバイスを使用する段階では、パスワード入力で通信許可とする通信認証装置の通信認証方法である。本実施例による通信認証方法は、使用者がパスワード入力で通信許可をもらう際に、通信認証装置から質問させる形式を、あらかじめ設定しておくステップと、複数の無線デバイスを、パスワードを用いて登録する時、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして入力するステップと、入力したパスワードを通信認証装置のメモリ部に記憶するステップと、複数の無線デバイスを通信エリア内で通信可能にする際、あらかじめ使用者が設定した質問形式で質問される内容の回答を、通信認証装置にデータ入力するステップと、入力したデータと通信認証装置のメモリ部に記憶された使用者の個人データを比較するステップと、比較した結果が一致した場合には通信を許可し、複数の無線デバイスを使用可能とするステップとを有する。本実施例によれば、通信エリア内で使用するデバイスの装置アドレスの他に、使用者自身に由縁のある氏名、生年月日、電話番号、電子メールアドレス、免許証番号等の情報をパスワードとして登録するので、忘却する危険性が少なく、パスワードを書き留める必要がない。また、使用認証時のパスワード入力は、あらかじめ使用者が定義しておいた質問形式に対して、複数個の答えを手動で入力するので使用者本人であれば正解を入力できるので、第三者による通信認証装置の不正使用の防止策となる。また、本実施例では、パスワードは、手動入力で説明したが、音声認識による入力方法であってもよい。

【００４８】図１８に記載の通信認証方法は、まず使用者がパスワード入力で通信許可をもらう際に、通信認証装置から質問させる形式を、あらかじめ設定しておき（Ｓ１７１）、複数の無線デバイスを、パスワードを用いて登録する時、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして入力し（Ｓ１７２）、入力したパスワードを通信認証装置のメモリ部に記憶する（Ｓ１７３）。次に、複数の無線デバイスを通信エリア内で通信可能にする際は、あらかじめ使用者が設定した質問形式で質問される内容の回答が、デバイスから自動的に通信認証装置１に対して送信され（Ｓ１８４）、複数の無線デバイスを使用可能とする（Ｓ１７６）。

【００４９】本実施例による通信認証方法は、複数の無線デバイスを特定の無線通信エリアで取り扱う通信シス

テムにおいて、複数の無線デバイスをパスワードで登録し、しかる後に複数の無線デバイスを使用する段階では、パスワード入力で通信許可とする通信認証装置の通信認証方法である。本実施例による通信認証方法は、使用者が、パスワード入力で通信許可をもらう際に、通信認証装置から質問させる形式を、通信認証装置にあらかじめ設定しておくステップと、複数の無線デバイスを、パスワードを用いて登録する時、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして入力するステップと、入力したパスワードを通信認証装置のメモリ部に記憶するステップと、使用者が、通信認証装置を特定の無線通信エリアに持ち込んだ時は、自動的にあらかじめ使用者が設定した質問形式で質問される内容の回答を、通信認証装置にデータ入力されるステップと、入力したデータと通信認証装置のメモリ部に記憶された使用者の個人データを比較するステップと、比較した結果が一致した場合には通信を許可し、複数の無線デバイスを使用可能とするステップとを有する。本実施例によれば、通信エリア内で使用するデバイスの装置アドレスの他に、使用者自身に由縁のある氏名、生年月日、電話番号、電子メールアドレス、免許証番号等の情報をパスワードとして登録するので、忘却する危険性が少なく、パスワードを書き留める必要がない。また、通信認証装置を特定の無線通信エリアに持ち込んだ時は、自動でパスワード入力されるので、通信認証装置の存在を意識することなく快適にセキュリティを保持できる。

【００５０】図１９に記載の通信認証方法は、まず使用者がパスワード入力で通信許可をもらう際に、通信認証装置から質問させる形式を、あらかじめ設定しておき（Ｓ１７１）、複数の無線デバイスを、パスワードを用いて登録する時、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして入力し（Ｓ１７２）、入力したパスワードを通信認証装置のメモリ部に記憶する（Ｓ１７３）。次に、使用者が特定の無線通信エリアに進入した時、鍵を挿入、又は使用されたことを検出し（Ｓ１９１）、あらかじめ使用者が設定した質問形式で質問される内容の回答を、デバイスから通信認証装置１にデータを入力して送信し（Ｓ１７４）、入力によって回答したデータと通信認証装置１のメモリ部７に記憶された使用者の個人データを比較し（Ｓ１７５）、比較した結果が一致した場合には通信を許可し、複数の無線デバイスを使用可能とする（Ｓ１７６）。また、本実施例では、固定された場所に設置してある通信認証装置で認証を行う場合の他、自動車等の移動するエリア内に通信認証装置が設置されている場合の認証であってもよい。また、通信認証装置を持ち歩いている場合であってもよい。また、本実施例では、Ｓ１７４での質問の回答を使用者が入力したが、自動入力であれば更に素早く認証が行える。

【００５１】本実施例による通信認証方法は、使用者が特定の無線通信エリアに進入した時の、特定無線通信エリアの認識と確定には、通信認証装置に鍵を挿入するか、あるいは鍵が特定場所で使用されたことを検出した電気信号による位置検出手段を利用するものである。本実施例によれば、家屋のドアロックシステムとの連動や、鍵による集中管理システムに利用することができる。また、通信認証装置が設置されている場合でも、通信認証装置を持ち歩いている場合でも、鍵の使用という別の目的のための動作の２次的な作用によって、その通信エリアが特定されて通信認証が開始されるので、通信認証装置の存在を意識することなく強固にセキュリティを保持できる。また、特定の無線通信エリアは、自動車の室内等の移動する空間であっても、鍵の使用によって確実に通信認証ができる。

【００５２】図２０に記載の通信認証方法は、使用者がパスワード入力で通信許可をもらう際に、通信認証装置から質問させる形式を、あらかじめ設定しておき（Ｓ１７１）、複数の無線デバイスを、パスワードを用いて登録する時、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして入力し（Ｓ１７２）、入力したパスワードを通信認証装置のメモリ部に記憶する（Ｓ１７３）。次に、使用者が特定の無線通信エリアに進入した時、鍵の挿入、又は使用されたことを検出後、通信認証装置をスタンバイモードから起動状態にし（Ｓ２０１）、あらかじめ使用者が設定した質問形式で質問される内容の回答を、デバイスから通信認証装置１にデータを入力して送信し（Ｓ１７４）、入力によって回答したデータと通信認証装置１のメモリ部７に記憶された使用者の個人データを比較し（Ｓ１７５）、比較した結果が一致した場合には通信を許可し、複数の無線デバイスを使用可能とする（Ｓ１７６）。また、本実施例では、固定された場所に設置してある通信認証装置で認証を行う場合の他、自動車等の移動するエリア内に通信認証装置が設置されている場合の認証であってもよい。また、通信認証装置を持ち歩いている場合であってもよい。また、本実施例では、Ｓ１７４での質問の回答を使用者が入力したが、自動入力であれば更に素早く認証が行える。

【００５３】本実施例による通信認証方法は、使用者が特定の無線通信エリアに進入した時の、特定無線通信エリアの認識と確定には、通信認証装置に鍵を挿入するか、あるいは鍵が特定空間で使用されたことを検出した電気信号による位置検出手段を利用し、位置検出手段で検出した位置情報に基づいて、通信認証装置をスタンバイ状態から起動状態にするものである。本実施例によれば、通信認証装置が設置されている場合でも、通信認証装置を持ち歩いている場合でも、鍵の使用という別の目

的のための動作の２次的な作用によって、その通信エリアが特定されて通信認証装置が起動状態になるので、通信認証装置の存在を意識することなく強固にセキュリティを保持できる。また、通信認証装置の消費電力を減少させることができる。

【００５４】図２１に記載の通信認証方法は、まず使用者がパスワード入力で通信許可をもらう際に、通信認証装置から質問させる形式を、あらかじめ設定しておき（Ｓ１７１）、複数の無線デバイスを、パスワードを用いて登録する時、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして入力し（Ｓ１７２）、入力したパスワードを通信認証装置のメモリ部に記憶する（Ｓ１７３）。次に、使用者が通信認証装置を特定の無線通信エリアに持ち込んだ時は、通信認証装置に搭載されたＧＰＳやＰＨＳ等の位置検出手段を利用して位置を確定し（Ｓ２１１）、あらかじめ使用者が設定した質問形式で質問される内容の回答を、デバイスから通信認証装置１にデータを入力して送信し（Ｓ１７４）、入力によって回答したデータと通信認証装置１のメモリ部７に記憶された使用者の個人データを比較し（Ｓ１７５）、比較した結果が一致した場合には通信を許可し、複数の無線デバイスを使用可能とする（Ｓ１７６）。また、本実施例では、Ｓ１７４での質問の回答を使用者が入力したが、自動入力であれば更に素早く認証が行える。また、特定の無線通信エリアを複数登録しておけば、複数の場所での認証も可能になる。

【００５５】本実施例による通信認証方法は、使用者が通信認証装置を特定の無線通信エリアに持ち込んだ時の、特定無線通信エリアの認識と確定には、通信認証装置に搭載されたＧＰＳやＰＨＳ等の位置検出手段を利用するものである。本実施例によれば、使用者がＧＰＳやＰＨＳによる位置検出手段を搭載した通信認証装置を持ち歩き、その通信認証装置を使用者があらかじめ位置設定した場所（無線通信エリア）に持ち込んだ時のみ、パスワードによる通信認証が開始されるので、強固にセキュリティを保持できる。

【００５６】図２２に記載の通信認証方法は、まず使用者がパスワード入力で通信許可をもらう際に、通信認証装置から質問させる形式を、あらかじめ設定しておき（Ｓ１７１）、複数の無線デバイスを、パスワードを用いて登録する時、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして入力し（Ｓ１７２）、入力したパスワードを通信認証装置のメモリ部に記憶する（Ｓ１７３）。次に、使用者が通信認証装置を特定の無線通信エリアに持ち込んだ時は、通信認証装置に搭載されたＧＰＳやＰＨＳ等の位置検出手段を利用して位置を確定し、通信認証装置をスタンバイモードから起動状態にし（Ｓ２２１）、あらかじめ使用者が設定した質問形式で

質問される内容の回答を、デバイスから通信認証装置１にデータを入力して送信し（Ｓ１７４）、入力によって回答したデータと通信認証装置１のメモリ部７に記憶された使用者の個人データを比較し（Ｓ１７５）、比較した結果が一致した場合には通信を許可し、複数の無線デバイスを使用可能とする（Ｓ１７６）。また、本実施例では、Ｓ１７４での質問の回答を使用者が入力したが、自動入力であれば更に素早く認証が行える。また、特定の無線通信エリアを複数登録しておけば、複数の場所での認証も可能になる。

【００５７】本実施例による通信認証方法は、使用者が通信認証装置を特定の無線通信エリアに持ち込んだ時の、特定無線通信エリアの認識と確定には、通信認証装置に搭載されたＧＰＳやＰＨＳ等の位置検出手段を利用し、位置検出手段で検出した位置情報に基づいて、通信認証装置をスタンバイ状態から起動状態にするものである。本実施例によれば、使用者がＧＰＳやＰＨＳによる位置検出手段を搭載した通信認証装置を持ち歩き、その通信認証装置を使用者があらかじめ位置設定した場所（無線通信エリア）に持ち込んだ時のみ、通信認証装置が起動状態になるので、より強固にセキュリティを保持できる。

【００５８】上記実施例においてＳ１７４では、複数の無線デバイスを通信エリア内で通信可能にする際、あらかじめ使用者が設定したパスワードがランダムに質問されるものであってもよい。また、Ｓ１７６では、通信認証装置のタイマー手段であらかじめ設定した時間経過後に、通信を開始するものであってもよい。この場合には、通信エリア内のデバイスを認証した後、通信認証装置に設定されている時間経過後に通信を開始するので、会議室などでメンバーが集まり、会議スタート時点からのデータ交信となり、機密情報が事前に配布されることがない。また、Ｓ１７６では、通信開始した後、通信認証装置のタイマー手段であらかじめ設定した時間経過後に通信を強制終了させるものであってもよい。通信開始した後、通信認証装置のタイマー手段であらかじめ設定した時間経過後に、通信を強制終了させるものである。通信エリア内のデバイスを認証し通信を開始した後、通信認証装置に設定されている時間経過後に通信を終了するので、管理者（使用者）が通信エリアから離れる場合や、会議室などで会議終了後しばらくしてのデータ交信終了をしたい場合などに利用でき、機密情報が管理者（使用者）の意に反して配布されることがない。また、上記実施例による通信認証方法において、複数の無線デバイスを通信認証装置にパスワードで登録する時、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして入力し、入力したパスワードを通信認証装置のメモリ部に所定の暗号化アルゴリズムに基づいて、暗号化して記憶するものであってもよい。この場合には、通信認

証装置にデバイスや通信形態を登録するとき用いたパスワードが暗号化保存されているので、第三者による故意のパスワード盗み出しに対処できる。また、上記実施例による通信認証方法において、通信認証装置からランダムな組み合わせや順序でパスワードを出すことで、前回の通信認証のパスワード入力時に盗み見られた場合でも、強固にセキュリティを保持できる。また、本実施例による通信認証方法の全てか、あるいは単独、あるいは複数の組み合わせを備えたプロトコル制御プログラムを記録媒体に格納し、または通信網を介してダウンロードすることもできる。そしてこのプログラムをブルートゥースによる通信が可能なモバイルコンピュータやパームＯＳコンピュータにインストールまたはダウンロードすることにより、通信認証装置として使用することができる。なお、本実施例での「データ通信」とは、正式な使用者が意図した実データの交信であって、接続前のブルートゥース方式のモバイル端末や家電装置間の接続要求等の装置が勝手に行うプロトコルは含まない。

【００５９】図２３は、本発明の他の実施例による通信認証方法を示すブロック図である。本実施例は、第１のデバイス２がハンドセット等の通信機能を持った端末装置であり、第２のデバイス３がモバイルルーターであって、両者の接続認証を通信認証装置１で行うものである。ハンドセット２からモバイルルーター３に接続要求（Ｓ２３１）をすると、モバイルルーター３から通信認証装置１に接続確認の問い合わせが発行される（Ｓ２３２）。通信認証装置１はハンドセット２が使用者本人の所有物であり、かつ通信認証装置１も使用者本人の所有物である検証を指紋認証により実施し（Ｓ２３３）、認証結果をモバイルルーター３に通知する（Ｓ２３４）。ハンドセット２が使用者本人の所有物であり、かつ通信認証装置１も使用者本人の所有物である認証結果はモバイルルーターからインターネットを介して認証サーバ５８で再度検証され接続許可の通知が来る（Ｓ２３５）。モバイルルーター３は接続許可通知（Ｓ２３５）に基づいて、ハンドセット２との通信を開始する（Ｓ２３６）。そして、ハンドセット２は電話網５５を利用して通話（Ｓ２３７）できるようになる。なお、上記実施例では、通信認証装置１において、ハンドセット２が使用者本人の所有物であり、かつ通信認証装置１も使用者本人の所有物であることの検証を指紋認証により実施したが、指紋認証をしないで通信認証装置１内にあらかじめ格納されている個人情報のみの検証でも可能である。

【００６０】図２４は、本発明の他の実施例による通信認証方法を示すブロック図である。本実施例は、第１のデバイス２がメール端末やＷｅｂ端末等の通信機能を持った端末装置であり、第２のデバイス３がモバイルルーターであって、両者の接続認証を通信認証装置１で行うものである。メール端末／Ｗｅｂ端末２からモバイルルーター３に接続要求（Ｓ２４１）をすると、モバイルルーター３から通信認証装置１に接続確認の問い合わせが発行される（Ｓ２４２）。通信認証装置１はメール端末／Ｗｅｂ端末２が使用者本人の所有物であり、かつ通信認証装置１も使用者本人の所有物である検証を指紋認証により実施し（Ｓ２４３）、認証結果をモバイルルーター３に通知する（Ｓ２４４）。メール端末／Ｗｅｂ端末２が使用者本人の所有物であり、かつ通信認証装置１も使用者本人の所有物である認証結果はモバイルルーターからインターネットを介して認証サーバ５８で再度検証され接続許可の通知が来る（Ｓ２４５）。モバイルルーター３は接続許可通知（Ｓ２４５）に基づいて、メール端末２との通信を開始する（Ｓ２４６）。そして、メール端末／Ｗｅｂ端末２はインターネット５７に接続可能となる。なお、上記実施例では、通信認証装置１において、メール端末／Ｗｅｂ端末２が使用者本人の所有物であり、かつ通信認証装置１も使用者本人の所有物であることの検証を指紋認証により実施したが、指紋認証をしないで通信認証装置１内にあらかじめ格納されている個人情報のみの検証でも可能である。

【００６１】図２５は、本発明の他の実施例による通信認証方法を示すブロック図である。本実施例は、第１のデバイス２がリモコン装置であり、第２のデバイス３がモバイルルーターであり、第３のデバイス５９が表示装置であって、３者の接続認証を通信認証装置１で行うものである。リモコン２からモバイルルーター３に番組選択指示（Ｓ２５１）をすると、モバイルルーター３から通信認証装置１に使用者の番組視聴契約内容等の接続確認問い合わせが発行される（Ｓ２５２）。通信認証装置１はリモコン操作者の番組選択指示内容と、通信認証装置１内にあらかじめ格納されている番組視聴契約情報や個人情報の照合、および通信認証装置１がリモコン操作者本人の所有物である検証を指紋認証により実施し（Ｓ２５３）、認証結果をモバイルルーター３に通知する（Ｓ２５４）。リモコン２が操作者本人の所有物であり、かつ通信認証装置１も使用者本人の所有物である認証結果と選択された番組は、モバイルルーターからインターネットを介して認証サーバ５８で再度検証され接続許可の通知が来る（Ｓ２５５）。モバイルルーター３は接続許可通知（Ｓ２５５）に基づいて、放送局５４から供給される（Ｓ２５６）番組を表示装置５９に送信し（Ｓ２５７）、番組が表示装置５９に表示される。なお、上記実施例では、通信認証装置１において、リモコン２が操作者本人の所有物であり、かつ通信認証装置１も使用者本人の所有物であることの検証を指紋認証により実施したが、指紋認証をしないで通信認証装置１内にあらかじめ格納されている個人情報のみの検証でも可能である。

【００６２】図２６は、本発明の他の実施例による通信認証方法を示すブロック図である。本実施例は、第１のデバイス２がクレジットカードであり、第２のデバイス

３がレジスターであって、クレジットカード２で支払いをする際に、通信回線を使用して決済するための通信認証を通信認証装置１で行うものである。クレジットカードの情報を読み取りレジスター３へ通知すると（Ｓ２６１）、レジスター３から通信認証装置１へ、クレジットカード番号等のカードから読み取ったデータを送信する（Ｓ２６２）。通信認証装置１はクレジットカードが正当かつ有効な使用者本人の所有物であり、かつ通信認証装置１も使用者本人の所有物である検証を指紋認証により実施し（Ｓ２６３）、認証結果をレジスター３に通知する（Ｓ２６４）。クレジットカードが正当かつ有効な使用者本人の所有物であり、かつ通信認証装置１も使用者本人の所有物である認証結果はレジスターから通信回線を介してクレジットカードセンター６０に送信され（Ｓ２６５）、ここで初めてカード番号の照会を含めた詳細な検証された使用許可（決済許可）の通知が来る（Ｓ２６５）。レジスター３は使用許可（決済許可）の通知（Ｓ２４５）に基づいて、クレジットカードによる決済を行う。なお、上記実施例では、クレジットカード２は通常の磁気データ式のカードを想定しているが、ＩＣカードや無線通信可能なカード等でクレジットカードの機能を備えたものであってもよい。また、上記実施例において、クレジットカード２のクレジットカードセンター６０で再度行う際に、初めてカード番号の照会を含めた詳細な検証がされるので、販売店のレジスターにはカードの詳細情報は残存せず、極めて強固な機密保持が可能となる。なお、上記実施例におけるクレジットカードセンター６０は、クレジット以外のカードセンターであってもよい。

【００６３】図２７は、本発明の他の実施例による通信認証方法を示すブロック図である。本実施例は、第２のデバイス３が入場門や玄関扉等のゲートあり、ゲート３を開ける際に、通信回線を使用してゲートを開けるための認証を通信認証装置１で行うものである。ゲートを開ける希望者は、希望者個人が所有する通信認証装置１が正当かつ有効な使用者本人の所有物であることを、内部に予め格納されている個人情報を含めて指紋認証により検証を実施し（Ｓ２７１）、通信認証装置１からゲート３に、通信認証装置１の内部に予め格納されている個人情報や入門予約情報を通知する（Ｓ２７２）。ゲート３は通信認証装置から受け取ったデータを通信回線を介して認証サーバ５８に送信し（Ｓ２７３）、認証サーバ５８はゲートを開くためのデータとして有効であるか検証する。認証サーバ５８からゲート３に、ゲートオープン可能の通知が送られ（Ｓ２７４）、ゲート３はゲートを開ける（Ｓ２７５）。また、上記実施例において、認証サーバ５８で検証を行うにあたっては、利用者個人の指紋情報を扱うものではなく、通信認証装置１の内部に予め格納されている個人情報や入門予約情報の検証を行うものである。よって、指紋情報等の極めて機密性の高い

生体情報が外部に漏洩することはない。

【００６４】

【発明の効果】上記説明から明らかなように、本発明によれば、無線通信が可能なエリア内にある２台以上の通信装置とは別に存在する通信認証装置によって、エリア内にある２台以上の通信装置について通信を行うか否かを認証して通信を行うことができる。また、通信を行うか否かを認証方法として、個人の生体情報（指紋、角膜、遺伝子等）を利用することにより、より強固な機密保持が可能となる。また、通信機器間の通信機密保持のための暗号化手段と組み合わせて利用することにより、更に強固な機密保持が可能となる。

【図面の簡単な説明】

【図１】　本発明の一実施例による通信認証装置の機能ブロック図

【図２】　本発明の一実施例による通信認証装置の機能ブロック図

【図３】　本発明の一実施例による通信認証装置の機能ブロック図

【図４】　本発明の一実施例による通信認証方法を説明するための構成図

【図５】　本発明の一実施例による通信認証方法を説明するための構成図

【図６】　本発明の一実施例による通信認証方法を説明するための構成図

【図７】　本発明の一実施例による通信認証方法を説明するための構成図

【図８】　本発明の一実施例による通信認証方法を説明するための構成図

【図９】　本発明の一実施例による通信認証方法を説明するための構成図

【図１０】　本発明の一実施例による通信認証方法を説明するための構成図

【図１１】　本発明の一実施例による通信認証方法を説明するための構成図

【図１２】　本発明の一実施例による通信認証方法を説明するための構成図

【図１３】　本発明の一実施例による通信認証方法を説明するための構成図

【図１４】　本発明の一実施例による通信認証方法を説明するための構成図

【図１５】　本発明の一実施例による通信認証方法を説明するための構成図

【図１６】　本発明の一実施例による通信認証方法を説明するための構成図

【図１７】　本発明の一実施例によるパスワードによる通信認証方法を説明するフロー図

【図１８】　本発明の一実施例によるパスワードによる通信認証方法を説明するフロー図

【図１９】　本発明の一実施例によるパスワードによる

通信認証方法を説明するフロー図

【図２０】　本発明の一実施例によるパスワードによる通信認証方法を説明するフロー図

【図２１】　本発明の一実施例によるパスワードによる通信認証方法を説明するフロー図

【図２２】　本発明の一実施例によるパスワードによる通信認証方法を説明するフロー図

【図２３】　本発明の一実施例による通信認証方法を説明するための構成図

【図２４】　本発明の一実施例による通信認証方法を説明するための構成図

【図２５】　本発明の一実施例による通信認証方法を説明するための構成図

【図２６】　本発明の一実施例による通信認証方法を説明するための構成図

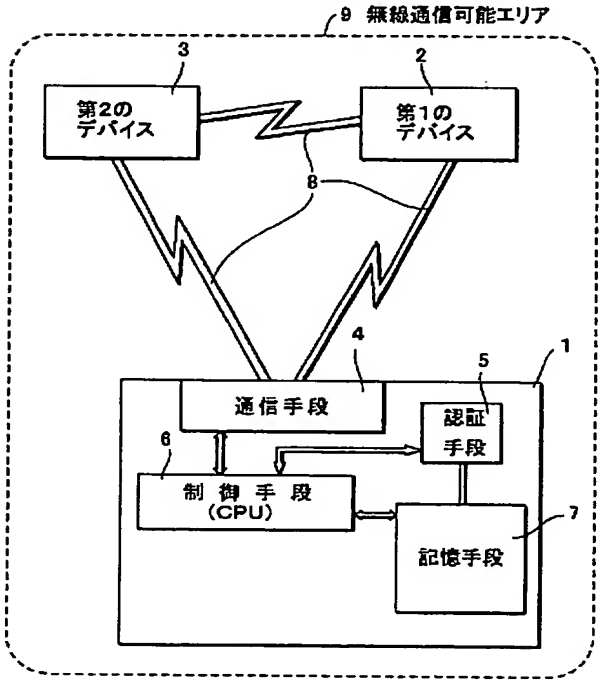
【図２７】　本発明の一実施例による通信認証方法を説明するための構成図

【符号の説明】

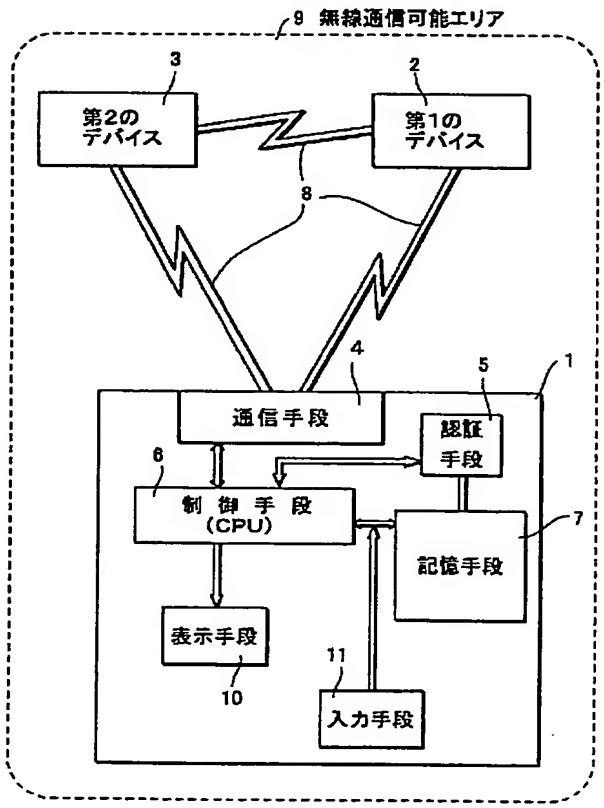
1　通信認証装置
2　第１のデバイス
3　第２のデバイス
4　通信手段
5　認証手段

6　制御手段
7　記憶手段
8　通信回線
9　無線通信可能エリア
１０　表示手段
１１　入力手段
１２　リムーバブルメモリ手段
１３　ホストインターフェイス手段
１４　起動手段
１５　位置情報検出手段
１６　タイマー手段
１７　外部入力端子
１８　表示出力手段
５１　ホストコンピュータ
５２　鍵
５３　外部入力装置
５４　放送局
５５　公衆網
５６　公衆網用ゲートウェイ
５７　インターネット
５８　認証サーバ
５９　第３のデバイス
６０　クレジットカードセンター

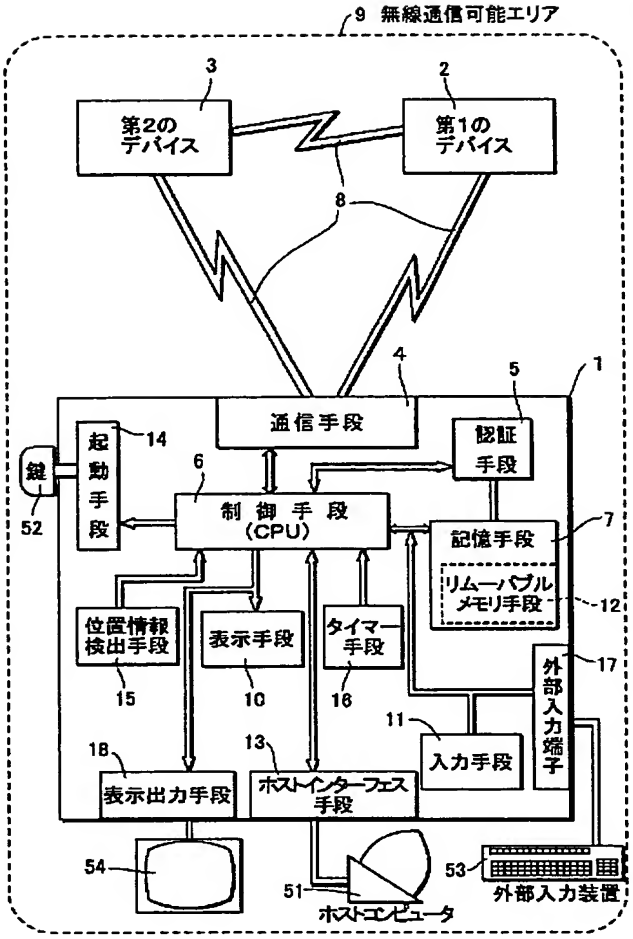
【図１】



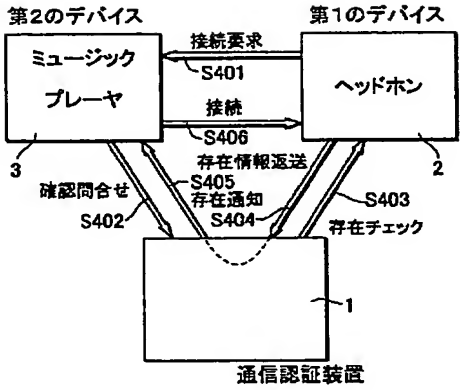
【図２】



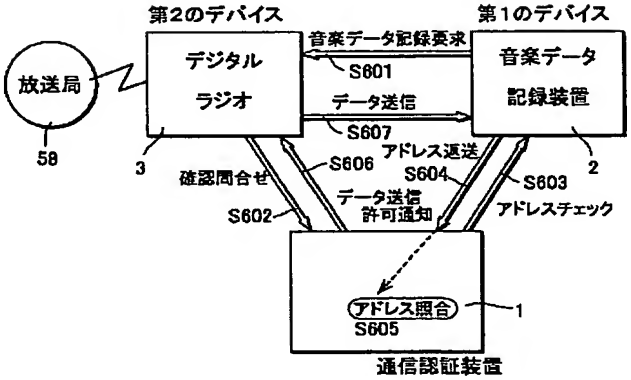
【図３】


9 無線通信可能エリア
第2のデバイス
第1のデバイス
8
通信手段
認証手段
起動手段
鍵
制御手段(CPU)
記憶手段
リムーバブルメモリ手段
位置情報検出手段
表示手段
タイマー手段
外部入力端子
入力手段
表示出力手段
ホストインターフェース手段
ホストコンピュータ
外部入力装置

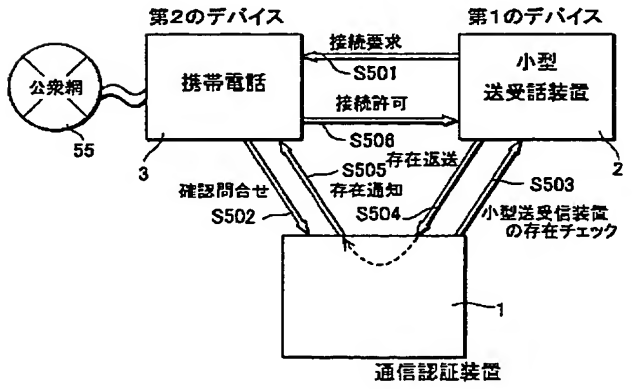
【図４】


第2のデバイス
第1のデバイス
ミュージックプレーヤ
ヘッドホン
接続要求
S401
接続
S406
存在情報返送
S405
確認問合せ
存在通知
S402
S404
S403
存在チェック
通信認証装置

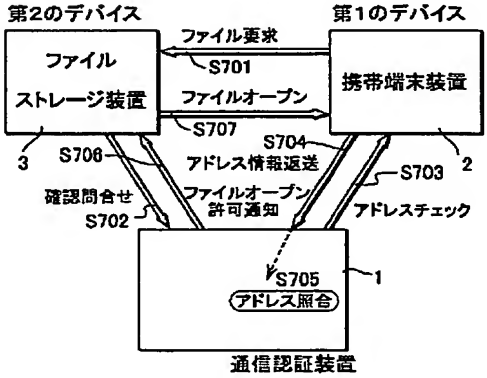
【図６】


第2のデバイス
第1のデバイス
放送局
デジタルラジオ
音楽データ記録装置
音楽データ記録要求
S601
データ送信
S607
アドレス返送
S606
S604
S603
確認問合せ
データ送信許可通知
S602
アドレスチェック
アドレス照合
S605
通信認証装置

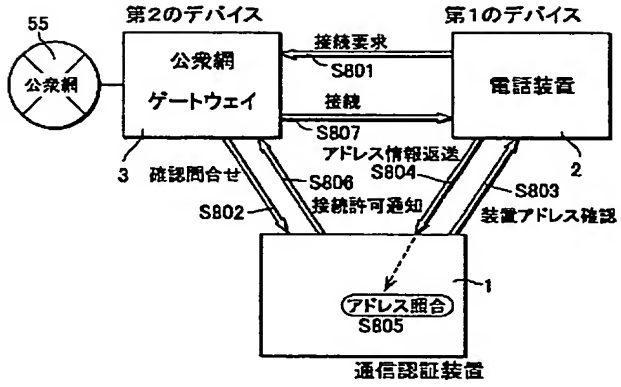
【図５】


第2のデバイス
第1のデバイス
公衆網
携帯電話
小型送受話装置
接続要求
S501
接続許可
S506
存在返送
S505
確認問合せ
存在通知
S502
S504
S503
小型送受信装置の存在チェック
通信認証装置

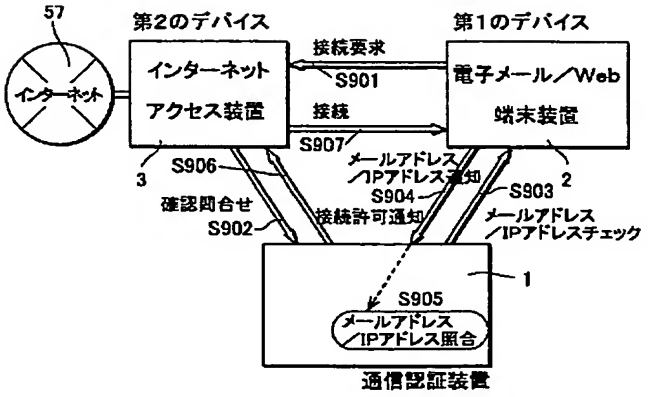
【図７】


第2のデバイス
第1のデバイス
ファイルストレージ装置
携帯端末装置
ファイル要求
S701
ファイルオープン
S707
S704
S706
アドレス情報返送
S703
確認問合せ
ファイルオープン許可通知
S702
アドレスチェック
S705
アドレス照合
通信認証装置

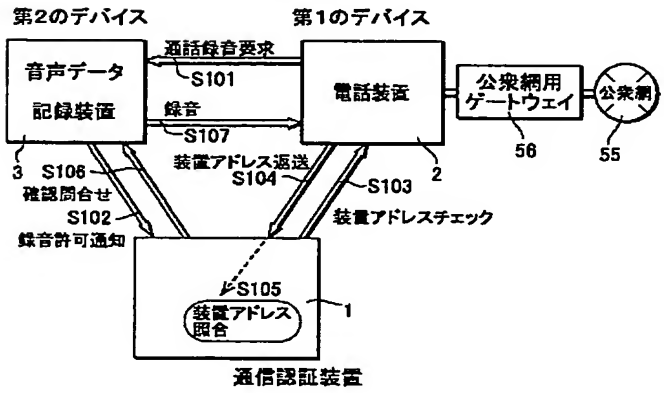
【図８】



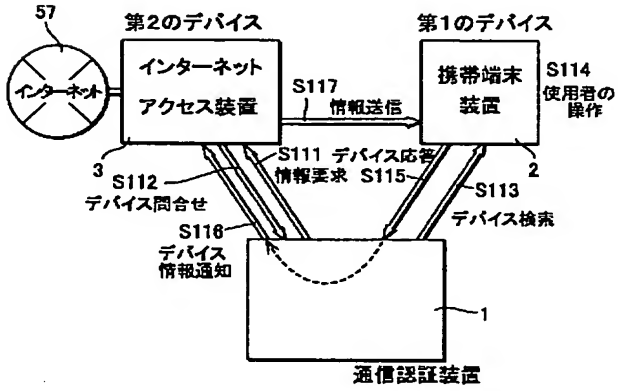
【図９】



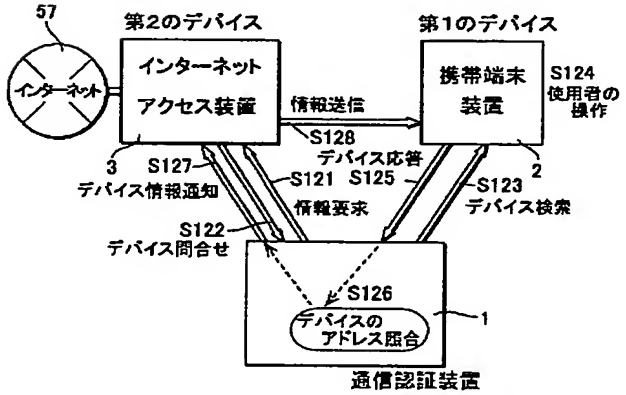
【図１０】



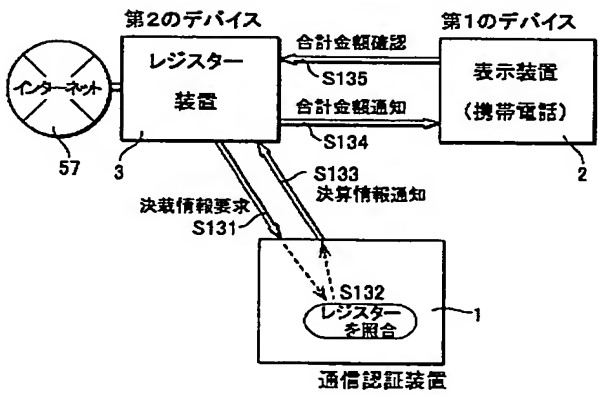
【図１１】



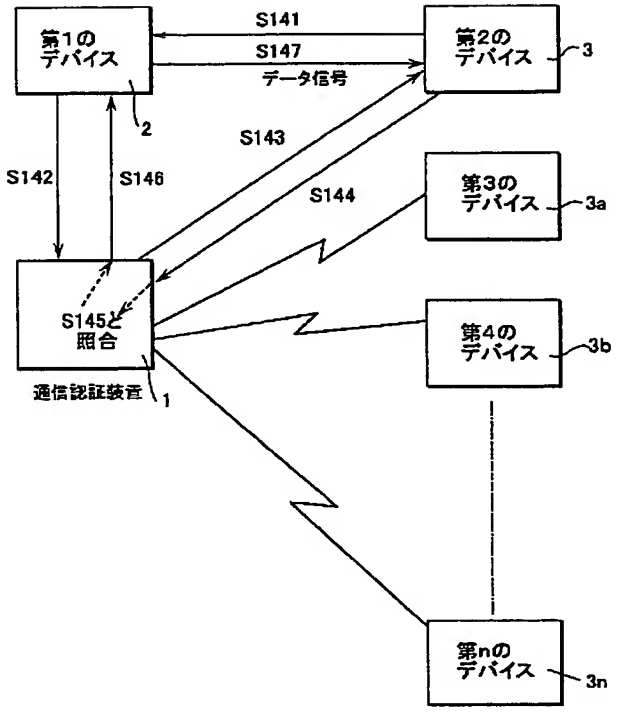
【図１２】



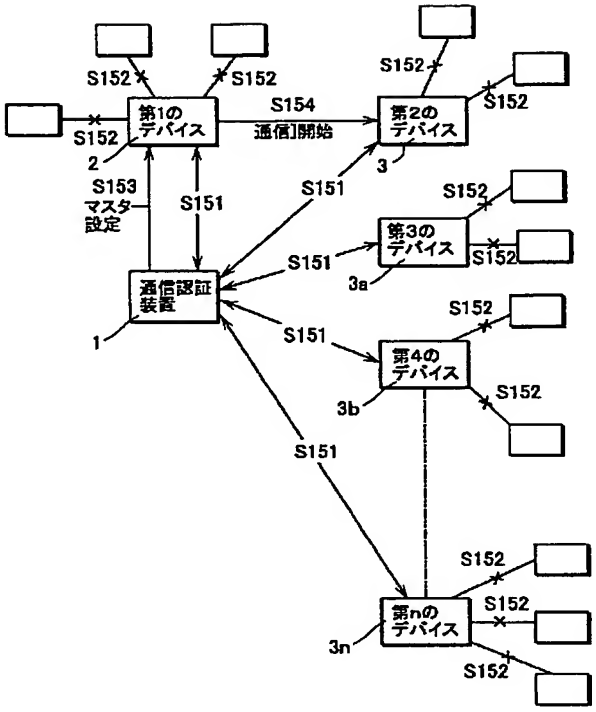
【図１３】



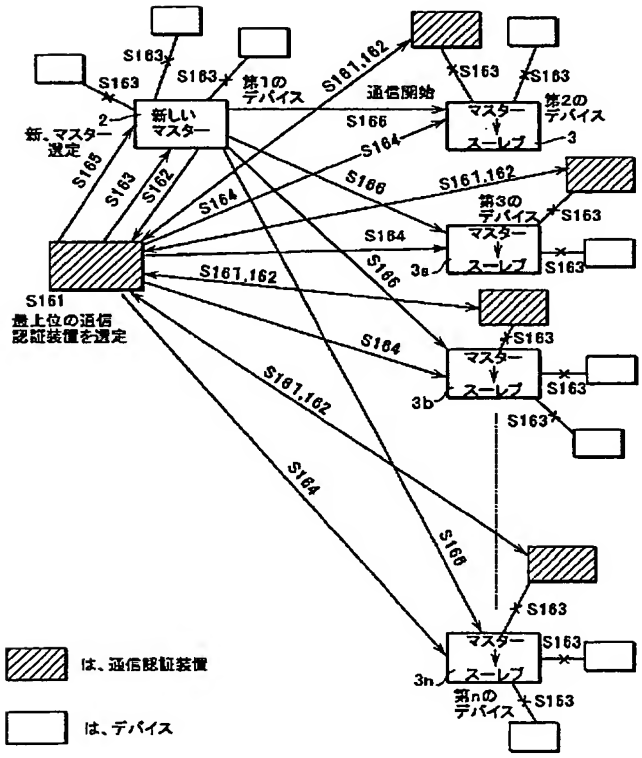
【図１４】



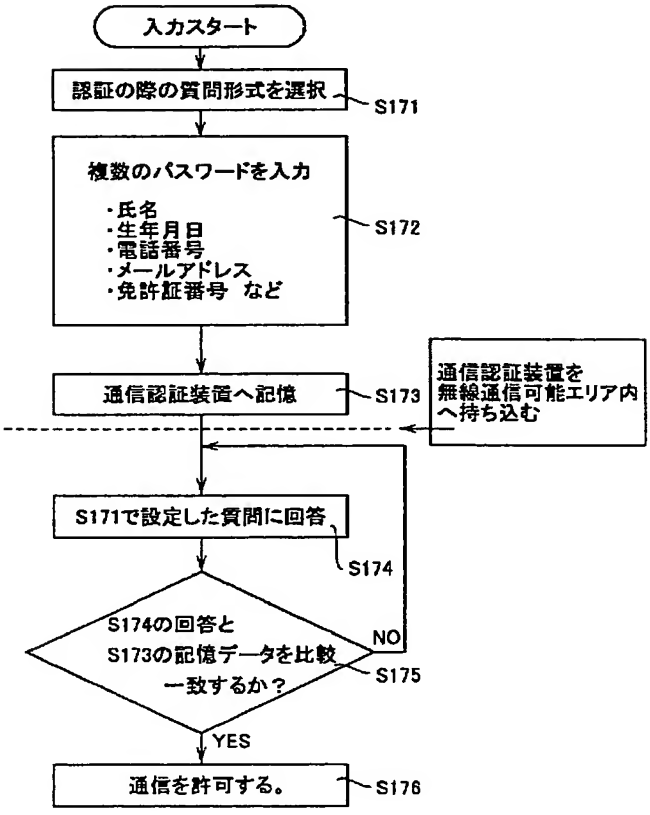
【図１５】



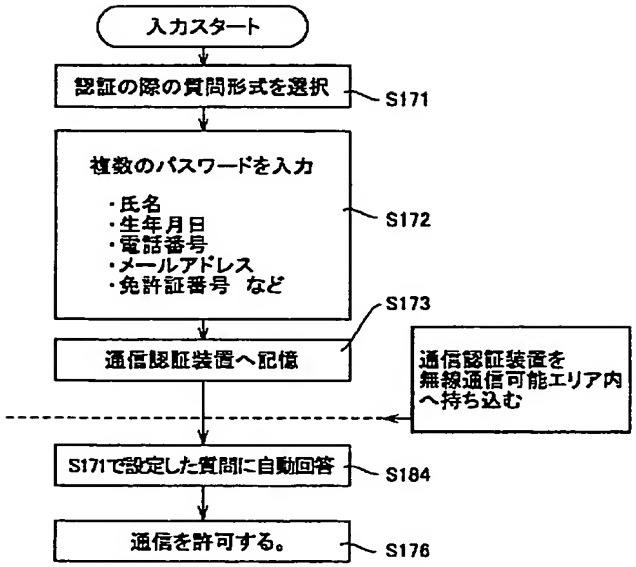
【図１６】



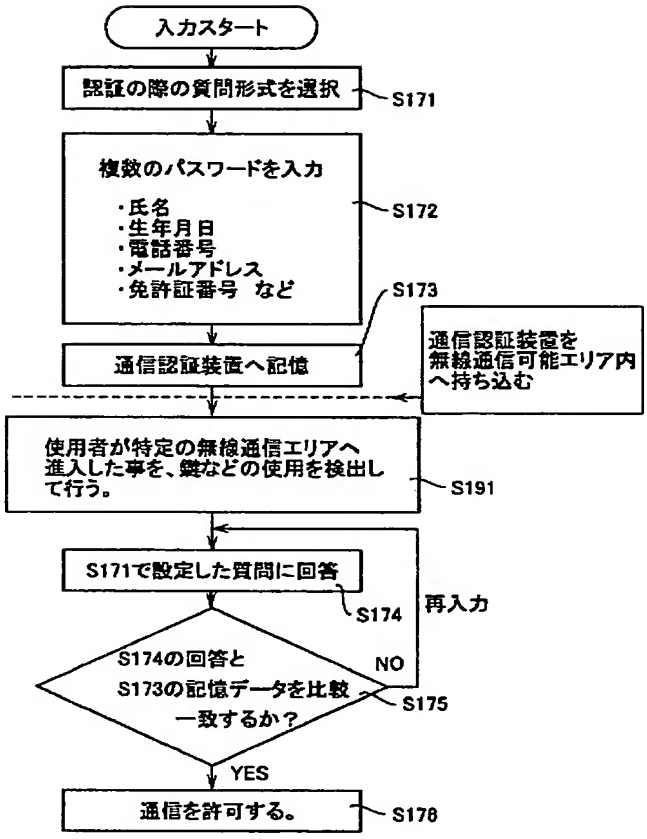
【図１７】



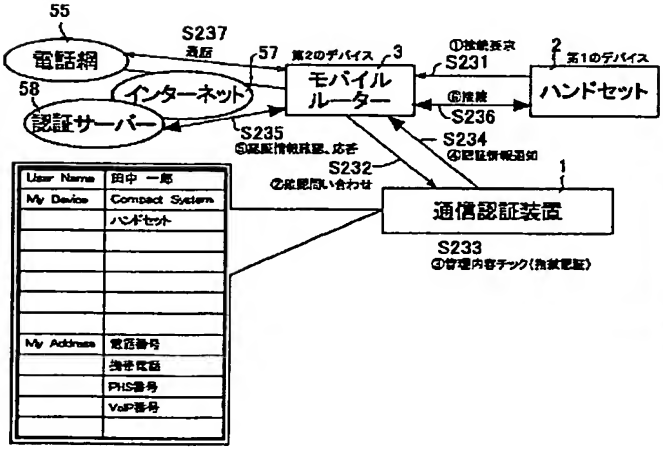
【図１８】



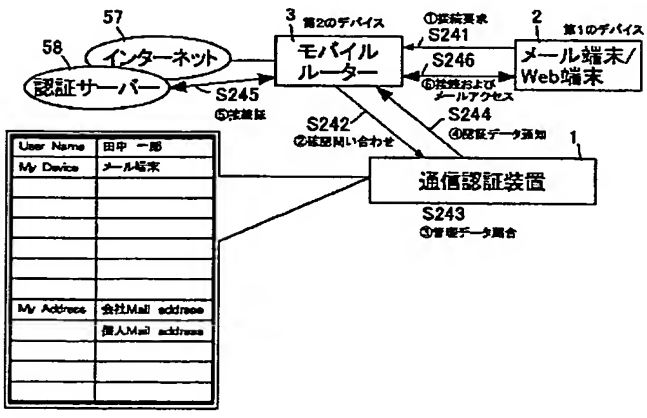
【図１９】



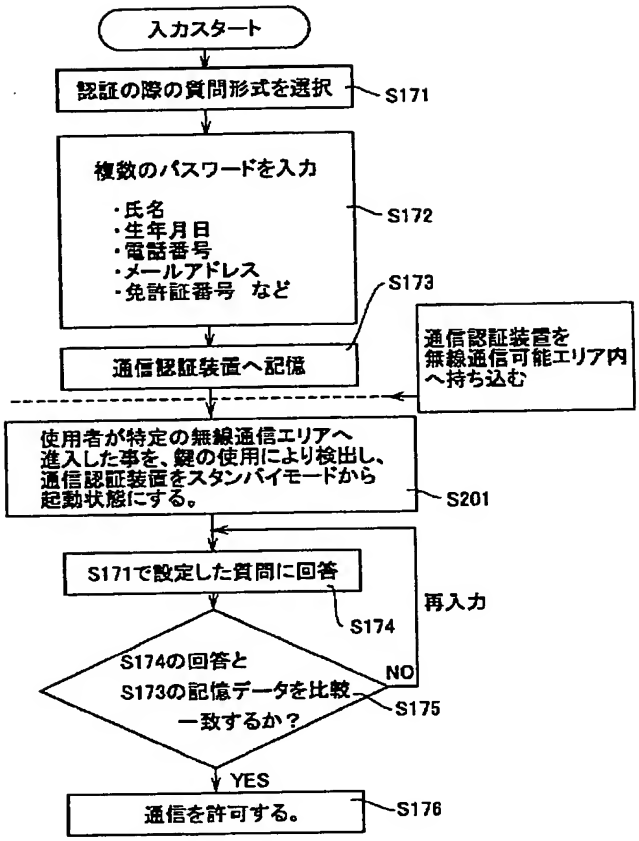
【図２３】



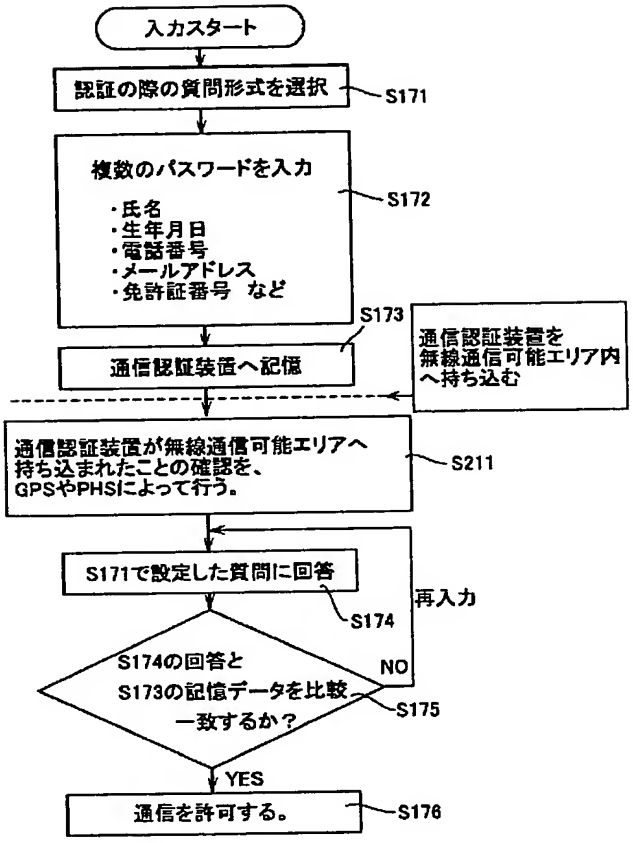
【図２４】



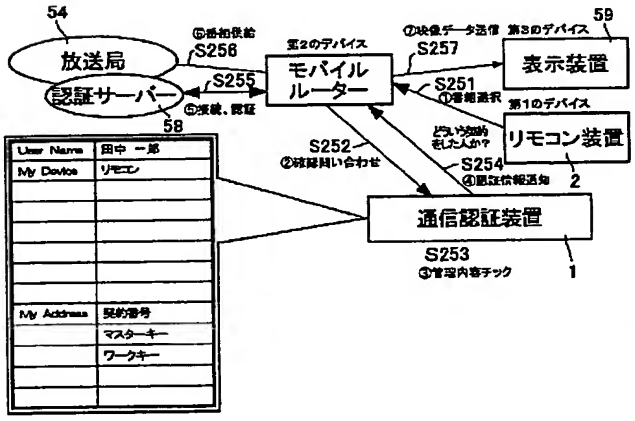
【図２０】



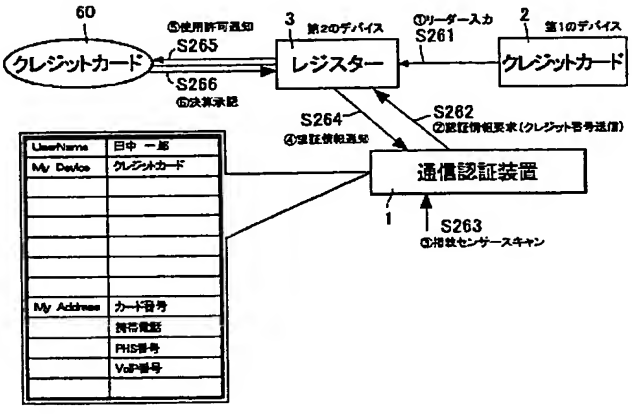
【図２１】



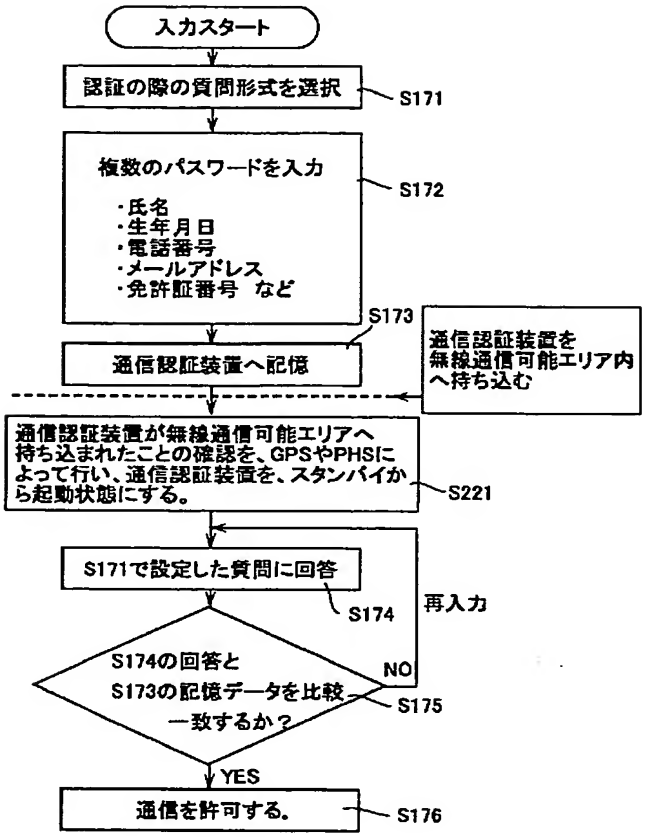
【図２５】



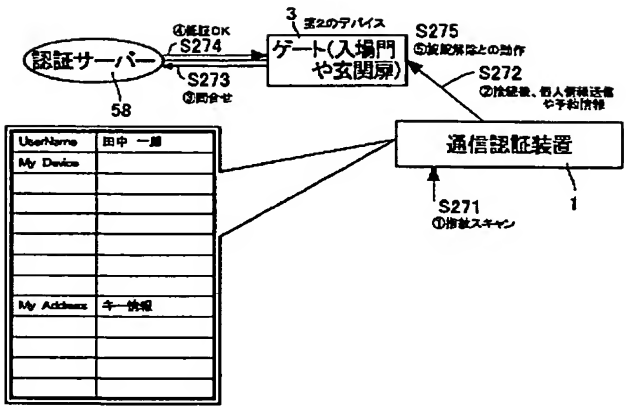
【図２６】



【図２２】



【図２７】



フロントページの続き

(72)発明者　松田　俊介
東京都品川区南大井６－17－17　ＦＩＮＥ
ビル　株式会社イーウィズユー内
(72)発明者　三室　悟
東京都品川区南大井６－17－17　ＦＩＮＥ
ビル　株式会社イーウィズユー内

Ｆターム(参考)　5B085 AA08 AE02 AE03 AE15 AE23
BC01 BE01 BE04 BG02
5J104 AA07 KA02 KA06 KA16 MA01
NA05 PA01 PA07
5K033 AA08 CB01 DA19 DB12 EC01
EC03
5K067 AA30 BB01 BB21 DD04 DD17
EE02 EE10 EE16 HH36 KK13
KK15